PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-032571

(43)Date of publication of application : 03.02.1998

(51)Int.Cl. H04L 9/32
G09C 1/00

(21)Application number : 08-186266

(22)Date of filing : 16.07.1996

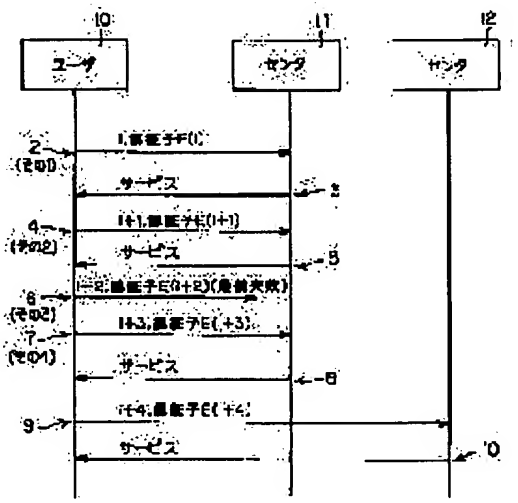
(71)Applicant : FUJITSU LTD

(72)Inventor : IWAYAMA NOBORU
HASEBE TAKAYUKI
TORII NAOYA
TAKENAKA MASAHIKO

(54) AUTHENTICATION SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To simply execute authentication processing while securing security by executing authentication processing based on a rule that a first authenticator included in first authentication information is the same authenticator as that signing a first code included in the first authentication information with a key.



SOLUTION: A center 11 checks whether or not the rule is conformed consisting of a first sub-rule that a counted value included in the authentication information transmitted this time (first authentication information) is larger than a counted value included in authentication information transmitted last time (second identification information), and a second sub-rule that an authenticator included in authentication information has a counted value included in the authentication information the same as that the authenticator which is signed with a key. Then at the time of obeying, the center 11 identifies that the call originating source of the identification information is correctly a user 10.

LEGAL STATUS

[Date of request for examination]	12.12.2002
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	3729940
[Date of registration]	14.10.2005
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－32571

(43)公開日　平成10年(1998)２月３日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ			技術表示箇所
Ｈ０４Ｌ	9/32			Ｈ０４Ｌ	9/00	６７５Ｄ	
Ｇ０９Ｃ	1/00	６４０	7259－5Ｊ	Ｇ０９Ｃ	1/00	６４０Ｅ	

審査請求　未請求　請求項の数11　ＯＬ　（全 12 頁）

(21)出願番号　特願平8－186266

(22)出願日　平成８年(1996)７月16日

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号

(72)発明者　岩山　登
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

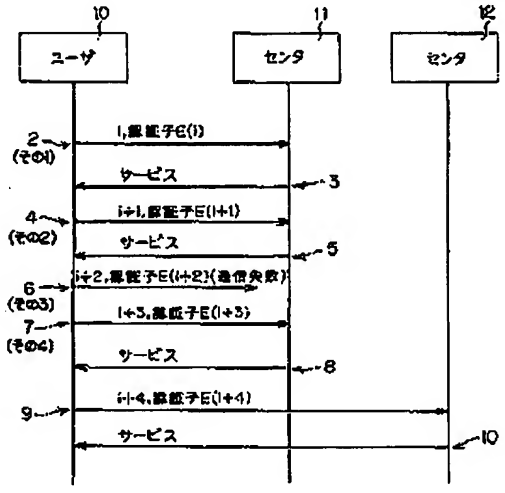
(72)発明者　長谷部　貢行
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

(74)代理人　弁理士　山田　正紀

最終頁に続く

(54)【発明の名称】　認証方式

(57)【要約】
【課題】十分な安全性を確保した上で認証処理を簡単に行なうことのできる認識方式を提供する。
【解決手段】ユーザ１０とセンタ１１，１２との双方でカウント値を保持し、直前に成功した認証の結果得られたユーザ１０のカウント値よりもセンタ１１，１２のカウント値の方が進んでいることに基づいて認証を行う。



1

【特許請求の範囲】

【請求項1】　送信されてきた情報に基づいて該情報が正当な発信元から送信されてきた情報であることの認証を行なうセンタと、該センタに向けて情報を送信し該情報が正当な発信元から発信された情報であることの認証を受けるユーザとの間での前記認証を実行する認証方式において、

前記ユーザと前記センタとの双方で、順序が定められた符号の集合を構成する該符号の順序を表わす情報と、符号に署名する鍵との双方を共有しておき、

前記ユーザは、前記認証を受けるにあたり、前記集合を構成する、認証を受けようとするたびに前記順序に従って更新してなる符号と、該符号に前記鍵で署名してなる認証子との双方からなる認証情報を前記センタに向けて送信し、

前記センタは、今回送信されてきた第1の認証情報に含まれる第1の符号が前記ユーザから前回送信されてきた第2の認証情報に含まれていた第2の符号よりも前記順序に従い後に位置する符号であるという第1のサブルールと、第1の認証情報に含まれる第1の認証子が、該第1の認証情報に含まれる第1の符号に前記鍵で署名してなる認証子と比べ同一の認証子であるという第2のサブルールとの双方のサブルールからなる第1のルールに従うか否かを調べ、該第1のルールに従っていた場合に、該第1の認証情報の発信元が正しく前記ユーザであることを認証することを特徴とする認証方式。

【請求項2】　送信されてきた情報に基づいて該情報が正当な発信元から送信されてきた情報であることの認証を行なうセンタと、該センタに向けて情報を送信し該情報が正当な発信元から発信された情報であることの認証を受けるユーザとの間での前記認証を実行する認証方式において、

前記ユーザと前記センタとの双方で、順序が定められた符号の集合を構成する該符号の順序を表わす情報と、符号に署名する鍵との双方を共有しておき、

前記ユーザは、前記認証を受けるにあたり、前記集合を構成する、認証を受けようとするたびに前記順序に従って更新してなる符号と、該符号と送信先のセンタを特定するセンタＩＤ符号とを結合してなる結合符号に前記鍵で署名してなる認証子との双方からなる認証情報を前記センタに向けて送信し、

前記センタは、今回送信されてきた第1の認証情報に含まれる第1の符号が前記ユーザから前回送信されてきた第2の認証情報に含まれていた第2の符号よりも前記順序に従い後に位置する符号であるという第1のサブルールと、第1の認証情報に含まれる第1の認証子が、該第1の認証情報に含まれる第1の符号と自分自身のセンタＩＤ符号とを結合してなる結合符号に前記鍵で署名してなる認証子と比べ同一の認証子であるという第2のサブルールとの双方のサブルールからなる第1のルールに従うか否かを調べ、該第1のルールに従っていた場合に、該第1の認証情報の発信元が正しく前記ユーザであることを認証することを特徴とする認証方式。

【請求項3】　前記センタは、前記第1のサブルールとして、前記第1の符号が前記第2の符号を起点とし前記順序に従い所定の範囲内に位置する符号であるという規則が付加されたサブルールを採用することを特徴とする請求項1又は2記載の認証方式。

【請求項4】　前記センタは、今回送信されてきた第1の認証情報が前記第2のサブルールに従っていなかった場合に不正な認証要求であると判定することを特徴とする請求項1又は2記載の認証方式。

【請求項5】　前記センタは、今回送信されてきた第1の認証情報が前記第2のサブルールには従っているものの前記第1のサブルールに従っていなかった場合に、該センタで発生させた乱数を前記ユーザに送信し、

前記ユーザは、前記センタから送信されてきた乱数に前記鍵で署名してなる第2の認証子を含む第3の認証情報を前記センタに向けて送信し、

前記センタは、今回送信されてきた第3の認証情報に含まれる第2の認証子が該センタで発生させた前記乱数に前記鍵で署名してなる認証子と比べ同一の認証子であるという第2のルールに従うか否かを調べ、該第2のルールに従っていた場合に、前回送信されてきた第1の認証情報及び今回送信されてきた第3の認証情報との双方の発信元が正しく前記ユーザであることを認証することを特徴とする請求項1又は2記載の認証方式。

【請求項6】　前記第3の認証情報が、前記集合を構成する符号のうちのいずれかの符号である第3の符号を含むものであることを特徴とする請求項5記載の認証方式。

【請求項7】　前記ユーザは、前記第2の認証子として、前記乱数と前記第3の符号とが結合されてなる結合符号に前記鍵で署名してなる認証子を前記センタに送信するものであり、

前記センタは、前記第2のルールとして、今回送信されてきた第3の認証情報に含まれる第2の認証子が、該センタで発生させた前記乱数と今回送信されてきた認証情報に含まれる第3の符号とが結合されてなる結合符号に前記鍵で署名してなる認証子と比べ同一の認証子であるというルールを採用するものであることを特徴とする請求項6記載の認証方式。

【請求項8】　送信されてきた情報に基づいて該情報が正当な発信元から送信されてきた情報であることの認証を行なうセンタと、該センタに向けて情報を送信し該情報が正当な発信元から発信された情報であることの認証を受けるユーザとの間での前記認証を実行する認証方式において、

前記ユーザと前記センタとの双方で、順序が定められた符号の集合を構成する該符号の順序を表わす情報と、符

号に署名する鍵との双方を共有しておき、
前記ユーザは、前記認証を受けるにあたり、前記集合を構成する、認証を受けようとするたびに前記順序に従って更新してなる符号に前記鍵で署名してなる認証子を含む認証情報を前記センタに向けて送信し、
前記センタは、今回送信されてきた第1の認証情報に含まれる第1の認証子が、前記ユーザから前回送信されてきた第2の認証情報に含まれていた第2の符号よりも前記順序に従い後に位置する符号であって、かつ、該第2の符号を起点とし前記順序に従い所定の範囲内に位置する符号それぞれに前記鍵で署名してなる各認証子のうちのいずれかの認証子と同一の認証子であるという第1のルールに従っていた場合に、該第1の認証情報の発信元が正しく前記ユーザであることを認証することを特徴とする認証方式。
【請求項9】　送信されてきた情報に基づいて該情報が正当な発信元から送信されてきた情報であることの認証を行なうセンタと、該センタに向けて情報を送信し該情報が正当な発信元から発信された情報であることの認証を受けるユーザとの間での前記認証を実行する認証方式において、
前記ユーザと前記センタとの双方で、順序が定められた符号の集合を構成する該符号の順序を表わす情報と、符号に署名する鍵との双方を共有しておき、
前記ユーザは、前記認証を受けるにあたり、前記集合を構成する、認証を受けようとするたびに前記順序に従って更新してなる符号と送信先のセンタを特定するセンタID符号とを結合してなる結合符号に前記鍵で署名してなる認証子を含む認証情報を前記センタに向けて送信し、
前記センタは、今回送信されてきた第1の認証情報に含まれる第1の認証子が、前記ユーザから前回送信されてきた第2の認証情報に含まれていた第2の符号よりも前記順序に従い後に位置する符号であって、かつ、該第2の符号を起点とし前記順序に従い所定の範囲内に位置する符号それぞれと自分自身のセンタID符号とを結合してなる結合符号それぞれに前記鍵で署名してなる各認証子のうちのいずれかの認証子と同一の認証子であるという第1のルールに従っていた場合に、該第1の認証情報の発信元が正しく前記ユーザであることを認証することを特徴とする認証方式。
【請求項10】　前記ユーザは、現在時刻を知る第1の時計を有し、該ユーザは、前記集合を構成する符号として該時計から得られる現在時刻を表わす符号を用いるものであることを特徴とする請求項1又は7記載の認証方式。
【請求項11】　前記センタは、現在時刻を知る第2の時計を有し、該センタは、今回送信されてきた第1の認証情報が前記第1のルールに従うとともに、さらに、該第1の認証情報に含まれる第1の符号が表わす現在時刻

の、前回送信されてきた第2の認証情報に含まれる第2の符号が表わす現在時刻からの第1の経過時間が、前記第2の時計から得られた、今回送信されてきた第1の認証情報の受信時刻の、前回送信されてきた第2の認証情報の受信時刻からの第2の経過時間と比べ、所定の許容誤差以内にある場合に、該第1の認証情報の発信元が正しく前記ユーザであることを認証することを特徴とする請求項10記載の認証方式。
【発明の詳細な説明】
【0001】
【発明の属する技術分野】本発明は、送信されてきた情報に基づいてその情報が正当な発信元から送信されてきた情報であることの認証を行なうセンタと、そのセンタに向けて情報を送信しその情報が正当な発信元から発信された情報であることの認証を受けるユーザとの間での認証を実行する認証方式に関する。
【0002】
【従来の技術】従来より、上述のような認証方式として、以下のタイプ（型）の認証方式が知られている。
1）パスワード型の認証方式
ユーザは、センタにパスワードを予め登録しておき、認証を受けるにあたり、そのパスワードをセンタに向けて送信する。センタでは、送信されてきたパスワードが予め登録されているパスワードと一致した場合にそのパスワードの発信元が正しいユーザであることを認証する。この方式は、そのパスワードが悪意の第三者に盗聴された場合、その悪意の第三者による、センタへの不正なアクセスを許す結果となる。
2）追番型の認証方式
ユーザとセンタとの双方で、カウンタ（このカウンタは単調増加数列のものであればよく、例えば時刻を用いてもよい）を有し、ユーザは認証を受けるにあたり、ユーザ側のカウンタの値をセンタに向けて送信する。センタでは、送信されてきたカウンタの値とセンタ側のカウンタの値とが一致した場合にそのカウンタの値の発信元が正しいユーザであることを認証する。この方式では、カウンタの値ないし時刻が、ユーザとセンタとで完全に一致している必要があり、ユーザがセンタをアクセスしようとして失敗した場合や、複数のセンタをアクセスした場合等にカウンタの値が異なってしまう恐れがあり、また時刻を採用したときは、ユーザの時計とセンタの時計が完全に一致している必要がある。また、送信したカウンタの値が盗聴され、直ちに次のカウンタの値を生成して送信する等により、不正なアクセスを許す結果となる。
3）追番署名型の認証方式
ユーザとセンタとの双方にカウンタを有する。またユーザは、カウンタの値を暗号化する鍵を有するとともに、センタにその鍵を予め登録しておく。ユーザは認証を受けるにあたり、ユーザ側のカウンタの値をその鍵で署名

（認証子）を作成し、その署名をセンタに向けて送信する。一方、センタではセンタ側のカウンタの値に．登録されている鍵で署名し、作成した署名（認証子）とユーザから送信されてきた署名とが一致した場合にその署名の発信元が正しいユーザであることを認証する。ここで．ユーザ側のカウンタの値とセンタ側のカウンタの値は認証を行なう度にインクリメントされる。この方式の場合．盗聴されてもカウンタの値は知られないためその点ではかなり安全性は高まるが、カウンタの値を常に一致させておく必要があること等の問題が残っている。

４）チャレンジ・レスポンス型の認証方式

図５は、従来のチャレンジ・レスポンス型の認証方式の流れを示す図である。

【０００３】図５に示すユーザ４０は．乱数Ｒに署名する鍵を有するとともにセンタ４１にその鍵を登録しておく。先ず、ユーザ４０がサービス要求をセンタ４１に向けて送信する。すると、センタ４１はこのサービス要求を受けて、認証するにあたり、ユーザ４０に向けて乱数Ｒを送信する。ユーザ４０は、送信されてきた乱数Ｒにそのユーザ４０が有する鍵で署名して認証子Ｅ（Ｒ）（乱数Ｒの署名）を作成し．その認証子Ｅ（Ｒ）をセンタ４１に向けて送信する。一方、センタ４１でもその乱数Ｒに、登録されている鍵で署名して認証子を作成し、作成した認証子とユーザ４０から送信されてきた認証子Ｅ（Ｒ）とが一致した場合にその認証子Ｅ（Ｒ）の発信元が正しいユーザ４０であることを認証し、そのユーザ４０にサービスを提供する。この方式の場合、予測不能な乱数に鍵で署名することから悪意の第三者に対する安全性は一層高められている。

【０００４】上述した４種類の認証方式では、認証のために送信されるメッセージの予測は．パスワード型，追番型、追番署名型，チャレンジ・レスポンス型の順に困難になる。このため、不正なユーザによるセンタへの不正なアクセスに対する安全性は、パスワード型、追番型、追番署名型、チャレンジ・レスポンス型の順に高まる。このため．従来、チャレンジ・レスポンス型の認証方式が多く用いられている。

【０００５】一方、認証処理は、パスワード型、追番型、追番署名型、チャレンジ・レスポンス型の順にだんだんと複雑になる。このため、何回もの認証処理が連続的に必要となる場合、チャレンジ・レスポンス型の認証方式と同程度の安全性を確保しつつ認証処理を簡略化する要求がでてきた。この要求を満たすために、特開平５－２１９０５３号公報に１つの提案がある。

【０００６】図６は、特開平５－２１９０５３号公報に提案されたチャレンジ・レスポンス型の認証方式の流れを示す図である。この認証方式では．認証処理を繰り返し行なうにあたり、ユーザ５０，センタ５１の双方で、ユーザ５０がｉ回目に作成した認証子（Ｅ（Ｒ））をｉ＋１回目の乱数Ｅ（Ｒ）として用いている。このため、

センタ５１はｉ＋１回目に乱数を送る必要がなくその分全体の処理が速く済み、前述した図４に示すチャレンジ・レスポンス型の認証方式の、単純な認証処理を繰り返す場合に比べても安全性が低下することはない。

【０００７】

【発明が解決しようとする課題】しかし、上述した、ｉ回目に作成した認証子をｉ＋１回目の乱数として用いるチャレンジ・レスポンス型の認証方式を用い、インターネットのような．認証子がセンタに必ずしも届く保証がない通信回線を使用して認証処理を繰り返し行なうと、認証子が乱れ．認証に失敗することがある。

【０００８】また、ＷＷＷ（Ｗｏｒｌｄ　Ｗｉｄｅ　Ｗｅｂ）などのように複数のセンタにランダムにアクセスするサービスにこの認証方式を用いると、ユーザは、送信した認証子をセンタ毎に記録しておく必要があり、このためユーザ側の機構が複雑になる。本発明は．上記事情に鑑み、十分な安全性を確保した上で簡単に認証処理を行なうことのできる認証方式を提供することを目的とする。

【０００９】

【課題を解決するための手段】上記目的を達成する本発明の認証方式のうちの第１の認証方式は、送信されてきた情報に基づいてその情報が正当な発信元から送信されてきた情報であることの認証を行なうセンタと．そのセンタに向けて情報を送信しその情報が正当な発信元から発信された情報であることの認証を受けるユーザとの間での上記認証を実行する認証方式において、上記ユーザと上記センタとの双方で．順序が定められた符号の集合を構成するそれらの符号の順序を表わす情報と．符号に署名する鍵との双方を共有しておき．上記ユーザは、上記認証を受けるにあたり．上記集合を構成する．認証を受けようとするたびに上記順序に従って更新してなる符号と．その符号に上記鍵で署名してなる認証子との双方からなる認証情報を上記センタに向けて送信し．上記センタは、今回送信されてきた第１の認証情報に含まれる第１の符号がそのユーザから前回送信されてきた第２の認証情報に含まれていた第２の符号よりも上記順序に従い後に位置する符号であるという第１のサブルールと、第１の認証情報に含まれる第１の認証子が、その第１の認証情報に含まれる第１の符号に上記鍵で署名してなる認証子と比べ同一の認証子であるという第２のサブルールとの双方のサブルールからなる第１のルールに従うか否かを調べ、その第１のルールに従っていた場合に、その第１の認証情報の発信元が正しく上記ユーザであることを認証することを特徴とする。

【００１０】また、上記目的を達成する本発明の第２の認証方式は、送信されてきた情報に基づいてその情報が正当な発信元から送信されてきた情報であることの認証を行なうセンタと、そのセンタに向けて情報を送信しその情報が正当な発信元から発信された情報であることの

認証を受けるユーザとの間での上記認証を実行する認証方式において、上記ユーザと上記センタとの双方で、順序が定められた符号の集合を構成するそれらの符号の順序を表わす情報と、符号に署名する鍵との双方を共有しておき、上記ユーザは、上記認証を受けるにあたり、上記集合を構成する、認証を受けようとするたびに上記順序に従って更新してなる符号と、その符号と送信先のセンタを特定するセンタＩＤ符号とを結合してなる結合符号に上記鍵で署名してなる認証子との双方からなる認証情報を上記センタに向けて送信し、上記センタは、今回送信されてきた第１の認証情報に含まれる第１の符号がそのユーザから前回送信されてきた第２の認証情報に含まれていた第２の符号よりも上記順序に従い後に位置する符号であるという第１のサブルールと、第１の認証情報に含まれる第１の認証子が、その第１の認証情報に含まれる第１の符号と自分自身のセンタＩＤ符号とを結合してなる結合符号に上記鍵で署名してなる認証子と比べ同一の認証子であるという第２のサブルールとの双方のサブルールからなる第１のルールに従うか否かを調べ、その第１のルールに従っていた場合に、その第１の認証情報の発信元が正しく上記ユーザであることを認証することを特徴とする。

【００１１】ここで、上記本発明の第１の認証方式ないし第２の認証方式において、上記センタは、上記第１のサブルールとして、上記第１の符号が上記第２の符号を起点とし上記順序に従い所定の範囲内に位置する符号であるという規則が付加されたサブルールを採用することが好ましい。また、上記センタでは、今回送信されてきた第１の認証情報が上記第２のサブルールに従っていなかった場合に不正な認証要求であると判定される。

【００１２】また、上記本発明の第１の認証方式および第２の認証方式において、上記センタは、今回送信されてきた第１の認証情報が上記第２のサブルールには従っているものの上記第１のサブルールに従っていなかった場合に、センタで発生させた乱数を上記ユーザに送信し、上記ユーザは、上記センタから送信されてきた乱数に上記鍵で署名してなる第２の認証子を含む第３の認証情報を上記センタに向けて送信し、上記センタは、今回送信されてきた第３の認証情報に含まれる第２の認証子がそのセンタで発生させた上記乱数に上記鍵で署名してなる認証子と比べ同一の認証子であるという第２のルールに従うか否かを調べ、この第２のルールに従っていた場合に、前回送信されてきた第１の認証情報及び今回送信されてきた第３の認証情報との双方の発信元が正しく上記ユーザであることを認証することが効果的である。

【００１３】この場合に、上記第３の認証情報が、上記集合を構成する符号のうちのいずれかの符号である第３の符号を含むものであることが好ましく、その場合にさらに、上記ユーザは、上記第２の認証子として、上記乱数と上記第３の符号とが結合されてなる結合符号に上記鍵で署名してなる認証子を上記センタに送信するものであり、上記センタは、上記第２のルールとして、今回送信されてきた第３の認証情報に含まれる第２の認証子が、そのセンタで発生させた上記乱数と今回送信されてきた認証情報に含まれる第３の符号とが結合されてなる結合符号に上記鍵で署名してなる認証子と比べ同一の認証子であるというルールを採用するものであることが好ましい。

【００１４】また、上記目的を達成する本発明の認証方式のうちの第３の認証方式は、送信されてきた情報に基づいてその情報が正当な発信元から送信されてきた情報であることの認証を行なうセンタと、そのセンタに向けて情報を送信しその情報が正当な発信元から発信された情報であることの認証を受けるユーザとの間での上記認証を実行する認証方式において、上記ユーザと上記センタとの双方で、順序が定められた符号の集合を構成するそれらの符号の順序を表わす情報と、符号に署名する鍵との双方を共有しておき、上記ユーザは、上記認証を受けるにあたり、上記集合を構成する、認証を受けようとするたびに上記順序に従って更新してなる符号に上記鍵で署名してなる認証子を含む認証情報を上記センタに向けて送信し、上記センタは、今回送信されてきた第１の認証情報に含まれる第１の認証子が、そのユーザから前回送信されてきた第２の認証情報に含まれていた第２の符号よりも上記順序に従い後に位置する符号であって、かつ、その第２の符号を起点とし上記順序に従い所定の範囲内に位置する符号それぞれに上記鍵で署名してなる各認証子のうちのいずれかの認証子と同一の認証子であるという第１のルールに従っていた場合に、その第１の認証情報の発信元が正しく上記ユーザであることを認証することを特徴とする。

【００１５】さらに、本発明の認証方式のうちの第４の認証方式は、送信されてきた情報に基づいてその情報が正当な発信元から送信されてきた情報であることの認証を行なうセンタと、そのセンタに向けて情報を送信しその情報が正当な発信元から発信された情報であることの認証を受けるユーザとの間での上記認証を実行する認証方式において、上記ユーザと上記センタとの双方で、順序が定められた符号の集合を構成するそれらの符号の順序を表わす情報と、符号に署名する鍵との双方を共有しておき、上記ユーザは、上記認証を受けるにあたり、上記集合を構成する、認証を受けようとするたびに上記順序に従って更新してなる符号と送信先のセンタを特定するセンタＩＤ符号とを結合してなる結合符号に前記鍵で署名してなる認証子を含む認証情報を上記センタに向けて送信し、上記センタは、今回送信されてきた第１の認証情報に含まれる第１の認証子が、そのユーザから前回送信されてきた第２の認証情報に含まれていた第２の符号よりも上記順序に従い後に位置する符号であって、かつ、その第２の符号を起点とし上記順序に従い所定の範

囲内に位置する符号それぞれと自分自身のセンタＩＤ符号とを結合してなる結合符号それぞれに上記鍵で署名してなる各認証子のうちのいずれかの認証子と同一の認証子であるという第１のルールに従っていた場合に、その第１の認証情報の発信元が正しく上記ユーザであることを認証することを特徴とする。

【００１６】ここで、上記本発明の第１～第４の認証方式において、上記ユーザは、現在時刻を知る第１の時計を有し、そのユーザは、上記集合を構成する符号としてその時計から得られる現在時刻を表わす符号を用いるものであってもよい。その場合に、さらに、上記センタは、現在時刻を知る第２の時計を有し、そのセンタは、今回送信されてきた第１の認証情報が上記第１のルールに従うとともに、さらに、その第１の認証情報に含まれる第１の符号が表わす現在時刻の、前回送信されてきた第２の認証情報に含まれる第２の符号が表わす現在時刻からの第１の経過時間が、上記第２の時計から得られた、今回送信されてきた第１の認証情報の受信時刻の、前回送信されてきた第２の認証情報の受信時刻からの第２の経過時間と比べ、所定の許容誤差以内にある場合に、その第１の認証情報の発信元が正しく上記ユーザであることを認証することが好ましい。

【００１７】

【発明の実施の形態】以下、本発明の実施形態について説明する。図１は、本発明の第１実施形態の認証方式におけるデータの流れを示す図である。尚、ここでは説明を容易にするために以下に記載する項目番号２～１０と同一の番号を、図１の、データの流れを示す矢印に付して説明する。

１．前提（この番号１は、図１には記入されていない）

図１に示すユーザ１０は、カウンタと、そのカウンタのカウント値に署名する鍵との双方を有する。このカウンタのカウント値は、本発明にいう符号に相当し、そのカウンタの一連のカウント値が、本発明にいう符号の集合に相当する。ここではこのカウンタの現在のカウント値がカウント値（ｉ）であるとする。またユーザ１０は、２つのセンタ１１，１２に、カウント値に署名する鍵を登録しておく。一方、センタ１１，１２は、ユーザ１０の、以前の認証処理によって得られたカウント値を保持している（ここでは、センタ１１のカウント値は（ｉ－１），センタ１２のカウント値（ｉ－２）であり、これらのカウント値は互いに異なっている）。このように、ここでは、ユーザ１０とセンタ１１、１２との双方で、ここで用いるカウンタがアップカウンタであるという情報（本発明にいう符号の順序を表す情報）、すなわちカウント値が順次インクリメントされるという情報と、カウント値に署名するための鍵との双方を共有している。

２．センタ１１への認証依頼（その１）

ユーザ１０は、認証を受けるにあたり、そのときのカウント値（ｉ）と、そのカウント値（ｉ）に鍵で署名してなる認証子Ｅ（ｉ）との双方からなる認証情報（ｉ，Ｅ（ｉ））をセンタ１１に向けて送信する。ユーザ１０は、その後、カウント値（ｉ）をインクリメントしてカウント値（ｉ＋１）とする。

３．センタ１１での認証処理

センタ１１は、今回送信されてきた認証情報（ｉ、Ｅ（ｉ））（本発明にいう第１の認証情報）に含まれるカウント値（ｉ）（本発明にいう第１の符号）が前回送信されてきた認証情報（ｉ－１，Ｅ（ｉ－１））（本発明にいう第２の認証情報）に含まれていたカウント値（ｉ－１）（本発明にいう第２の符号）よりも値の大きなカウント値であるという第１のサブルールと、認証情報（ｉ、Ｅ（ｉ））に含まれる認証子Ｅ（ｉ）が、その認証情報（ｉ，Ｅ（ｉ））に含まれるカウント値（ｉ）に鍵で署名してなる認証子Ｅ（ｉ）と比べ同一の認証子であるという第２のサブルールとの双方のサブルールからなるルール（本発明にいう第１のルール）に従うか否かを調べ、そのルールに従っていた場合に、その認証情報（ｉ、Ｅ（ｉ））の発信元が正しくユーザ１０であることを認証する。またセンタ１１は、ユーザ１０から受け取ったカウント値（ｉ）を記録する。さらにセンタ１１は、その認証情報の発信元が正当なユーザ１０であるので、そのユーザ１０にサービスを提供する。

４．センタ１１への認証依頼（その２）

ユーザ１０は、次の認証を受けるにあたり、カウント値（ｉ＋１）と、そのカウント値（ｉ＋１）に鍵で署名してなる認証子Ｅ（ｉ＋１）との双方からなる認証情報（ｉ＋１，Ｅ（ｉ＋１））をセンタ１１に向けて送信する。本発明と対比したとき、この認証情報（ｉ＋１，Ｅ（ｉ＋１））も本発明にいう第１の認証情報に相当する。ユーザ１０はその後カウント値（ｉ＋１）をインクリメントしてカウント値（ｉ＋２）とする。

５．センタ１１での認証処理

センタ１１は、今回送信されてきた認証情報（ｉ＋１，Ｅ（ｉ＋１））に含まれるカウント値（ｉ＋１）が前回送信されてきた認証情報（ｉ，Ｅ（ｉ））に含まれていたカウント値（ｉ）よりも値の大きなカウント値であるという第１のサブルールと、認証情報（ｉ＋１、Ｅ（ｉ＋１））に含まれる認証子Ｅ（ｉ＋１）が、その認証情報（ｉ＋１，Ｅ（ｉ＋１））に含まれるカウント値（ｉ＋１）に鍵で署名してなる認証子Ｅ（ｉ＋１）と比べ同一の認証子であるという第２のサブルールとの双方のサブルールからなるルール（本発明にいう第１のルール）に従うか否かを調べ、そのルールに従っていた場合に、その認証情報（ｉ＋１，Ｅ（ｉ＋１））の発信元が正しくユーザ１０であることを認証する。またセンタ１１は、ユーザ１０からのカウント値（ｉ＋１）を記録する。さらにセンタ１１は、その認証情報の発信元が正当なユーザ１０であるので、そのユーザ１０にサービスを提供する。

【００１８】ここまでで２回の認証処理を行ったが、単純にチャレンジ・レスポンス認証を２回繰り返すと、センタ１１からユーザ１０に乱数を送る必要上通信が８回必要となるところ、本実施形態の認証方式では４回の通信で済んでいる。次に、上述した処理に引き続き認証要求を行った結果、通信に失敗した場合について説明する。

6．センタ１１への認証依頼（その３）

ユーザ１０は、認証を受けるにあたり、カウント値（ｉ＋２）と、そのカウント値（ｉ＋２）に鍵で署名してなる認証子Ｅ（ｉ＋２）との双方からなる認証情報（ｉ＋２，Ｅ（ｉ＋２））をセンタ１１に向けて送信する。ユーザ１０はその後カウント値（ｉ＋２）をインクリメントしてカウント値（ｉ＋３）とする。しかし、この通信は失敗しセンタ１１からの応答がないので、ユーザの通信処理はタイムアウトとなり、あらためて認証を依頼する。

7．センタ１１への認証依頼（その４）

ユーザ１０は、認証を受けるにあたり、カウント値（ｉ＋３）と、そのカウント値（ｉ＋３）に鍵で署名してなる認証子Ｅ（ｉ＋３）との双方からなる認証情報（ｉ＋３，Ｅ（ｉ＋３））をセンタ１１に向けて送信する。尚、この認証情報（ｉ＋３，Ｅ（ｉ＋３））も本発明にいう第１の認証情報に相当する。ユーザ１０はその後カウント値（ｉ＋３）をインクリメントしてカウント値（ｉ＋４）とする。

8．センタ１１での認証処理

センタ１１は、今回送信されてきた認証情報（ｉ＋３，Ｅ（ｉ＋３））に含まれるカウント値（ｉ＋３）が前回送信されてきた認証情報（ｉ＋１，Ｅ（ｉ＋１））に含まれていたカウント値（ｉ＋１）よりも値の大きなカウント値であるという第１のサブルールと、認証情報（ｉ＋３，Ｅ（ｉ＋３））に含まれる認証子Ｅ（ｉ＋３）が、その認証情報（ｉ＋３，Ｅ（ｉ＋３））に含まれるカウント値（ｉ＋３）に鍵で署名してなる認証子Ｅ（ｉ＋３）と比べ同一の認証子であるという第２のサブルールとの双方のサブルールからなるルールに従うか否かを調べ、そのルールに従っていた場合に、その認証情報（ｉ＋３，Ｅ（ｉ＋３））の発信元が正しくユーザ１０であることを認証する。またセンタ１１は、その認証情報の発信元がユーザ１０からのカウント値（ｉ＋３）を記録する。さらにセンタ１１は、その認証情報の発信元が正当なユーザ１０であるので、そのユーザ１０にサービスを提供する。

【００１９】このように、認証情報（ｉ＋２，Ｅ（ｉ＋２））がセンタ１１に到着しなかった場合であっても、センタ１１において、次の認証情報（ｉ＋３，Ｅ（ｉ＋３））に含まれるカウント値（ｉ＋３）がセンタ１１に記録されているカウント値（ｉ＋１）より大きく、かつ、認証情報（ｉ＋３，Ｅ（ｉ＋３））に含まれる認証子（Ｅ（ｉ＋３））も、カウント値（ｉ＋３）に鍵で署名してなる認証子と同一の認証子であるため、認証に成功している。

【００２０】次に、上述した処理に引き続きセンタ１１とは異なるセンタであるセンタ１２に認証要求を行う場合について説明する。

9．センタ１２への認証依頼

ユーザ１０は、認証を受けるにあたり、カウント値（ｉ＋４）と、そのカウント値に鍵で署名してなる認証子Ｅ（ｉ＋４）との双方からなる認証情報（ｉ＋４，Ｅ（ｉ＋４））（この認証情報も本発明にいう第１の認証情報である）をセンタ１２に向けて送信する。ユーザ１０はその後カウント値（ｉ＋４）をインクリメントしてカウント値（ｉ＋５）とする。

１０．センタ１２での認証処理

センタ１２は、今回送信されてきた認証情報（ｉ＋４，Ｅ（ｉ＋４））に含まれるカウント値（ｉ＋４）が前回送信されてきた認証情報（ｉ－２，Ｅ（ｉ－２））に含まれていたカウント値（ｉ－２）よりも値の大きなカウント値であるという第１のサブルールと、認証情報（ｉ＋４，Ｅ（ｉ＋４））に含まれる認証子Ｅ（ｉ＋４）が、その認証情報（ｉ＋４，Ｅ（ｉ＋４））に含まれるカウント値（ｉ＋４）に鍵で署名してなる認証子（Ｅ（ｉ＋４））と比べ同一の認証子であるという第２のサブルールとの双方のサブルールからなるルール（本発明にいう第１のルール）に従うか否かを調べ、そのルールに従っていた場合に、その認証情報（ｉ＋４，Ｅ（ｉ＋４））の発信元が正しくユーザ１０であることを認証する。またセンタ１２は、ユーザ１０からのカウント値（ｉ＋４）を記録する。さらにセンタ１２は、その認証情報の発信元が正当なユーザ１０であるので、そのユーザ１０にサービスを提供する。

【００２１】このように、ユーザはセンタごとに認証子を変更する必要がなくどのセンタにアクセスする場合であっても同一の処理でよく、このため、ユーザ側の機構が簡単になる。図２は、図１に示す認証方式において、センタが認証依頼を受けた場合において、ユーザからのカウント値がセンタに記録されたカウント値よりも小さい場合の処理について示した図である。

【００２２】センタ１１は、認証子が正しくない場合（本発明にいう第２のサブルールを満足しない場合）は不正なアクセスと判断する。一方、認証子は正しいが、ユーザからのカウント値がセンタに記録されたカウント値よりも小さい（本発明にいう第１のサブルールを満足しない）場合は、ユーザ１０がカウンタを何らかの理由でリセットしたこともあり得るので、現在のカウント値をユーザ１０に問い合わせる。その問い合わせ手順について、図２を参照して説明する。以下に記載する項目番号１～４と同一の番号を図２に付して示す。

【００２３】１．センタ１１への認証依頼

ユーザ10は、認証を受けるにあたり、カウンタの値（i）と、そのカウンタの値（i）に鍵で署名してなる認証子E（i）との双方からなる認証情報（i，E i）（本発明にいう第1の認証情報）をセンタ11に向けて送信する。ユーザ10はその後カウントの（i）をインクリメントしてカウント値（i+1）にする。

【0024】2．センタ11での認証処理

センタ11では、今回送信されてきた認証情報（i，E（i））に含まれるカウント値（i）がそのセンタ11に記録されたカウント値（ここではそのセンタ11に記録されたカウント値はカウント値（i）よりも大きい値のカウント値であったとする）より小さいので、次に認証情報（i，E（i））に含まれるカウント値（i）に鍵で署名して認証子を作成し、作成された認証子がユーザ10からの認証子E（i）と一致しない場合、不正なアクセスであると判断し通信を終了する。一方、作成された認証子がユーザ10からの認証子E（i）と一致した場合、センタ11はそのセンタ11に備えられた乱数発生器（図示せず）によって任意に発生させた乱数Rをユーザ10に送信する。またこのときは、センタ11に記録されたカウント値（i－1）を保持したまま、今回のカウント値（i）を仮に記録する。

【0025】3．ユーザ10の応答

ユーザ10は、センタ11から送信されてきた乱数Rと、そのユーザ10が前回送信した認証情報（i，E（i））に含まれていたカウント値（i）よりも更新してなるカウント値（i+1）（本発明にいう第3の符号）とが結合されてなる結合符号に鍵で署名してなる認証子E（R，i+1）（本発明にいう第2の認証子の一例）と、そのカウント値（i+1）との双方からなる認証情報（i+1，E（R，i+1））（本発明にいう第3の認証情報）をセンタ11に向けて送信する。

【0026】4．センタ11での認証処理

センタ11は、今回送信されてきた認証情報（i+1，E（R，i+1））に含まれるカウント値（i+1）が前回送信されてきた認証情報（i，E（i））に含まれていたカウント値（i）よりも値の大きなカウント値であって、かつ今回送信されてきた認証情報（i+1，E（R，i+1））に含まれる認証子E（R，i+1）が、そのセンタ11で発生させた乱数Rと、今回送信されてきた認証情報（i+1，E（R，i+1））に含まれるカウント値（i+1）とが結合されてなる結合符号に鍵で署名してなる認証子と比べ同一の認証子であるというルール（本発明にいう第2のルールの一例）に従うか否かを調べ、そのルールに従っていた場合に、前回送信されてきた認証情報（i，E（i））及び今回送信されてきた認証情報（i+1，E（R，i+1））との双方の発信元が正しくユーザ10であることを認証し、サービスを提供する。また、このときユーザ10から送られたカウント値（i+1）を記録する。尚、そのルールに従っていない場合は不正なアクセスと判断し、仮に記録しておいたカウント値（i）を破棄し、その前に記録されていたカウント値（i－1）に戻す。

【0027】さらに引き続き、ユーザ10によるセンタ11への認証依頼（図2に示す番号5）が行われると、センタ11による、その認証依頼に対する認証処理（図2に示す番号6）が行われる。このように上述の第1実施形態の認証方式によれば、センタにおける認証は、直前の成功した認証の結果得られたユーザのカウント値より大きいカウント値に基づいてなされる。いいかえれば、本実施形態によれば必ずしも連続したカウント値から生成される認証子で認証する必要はなく、本実施形態はカウント値が進んでいることを認証する（もちろん、ユーザが鍵を持っていることも同時に認証する）認証方式であるため、認証子がセンタに必ず届く保証がなくても、余分な処理なしで、引き続き認証処理を行うことができる。

【0028】また、カウント値が進んでさえいればよいので、ユーザは送信した認証子をセンタごとに記録しておく必要がなく、異なるセンタにアクセスする場合でも同じ機構で認証依頼を行うことができる。さらに、上記の実施形態では、図2を参照して説明したようにカウンタの同期をとる機構を備えているため、安全性を高めるためにユーザのカウント値が変更された場合や、ユーザ側システムの再インストールなどによってユーザのカウンタの値が変更された場合にも容易に対処できる。

【0029】尚、上記第1の実施形態では、第1のサブルールとして、今回送信されてきた認証情報（例えば、認証情報（j，E（j））に含まれるカウント値（j）が前回送信されてきた認証情報（例えば認証情報（i，E（i））に含まれていたカウント値（i）よりも値の大きなカウント値（j＞i）であるというサブルールを採用したが、この第1のサブルールに、|j－i|が所定の範囲にある（|j－i|≦n）という規則を付加してもよい。こうすることにより、通信の安全性が一層高められる。また、上記の第1の実施形態では、ユーザからセンタに送信する認証情報には、カウント値（例えばカウント値（j））と、そのカウント値（j）に鍵で署名してなる認証子（例えばE（j））との双方が含まれているが、この第1の実施形態の変形例として、ユーザからセンタに向けて、カウント値（例えばカウント値（j））自身は送信せずに、その認証子（例えばE（j））のみを送信し、センタでは、そのユーザから前回送信されてきた認証子（例えばE（i））に対応して記憶しておいたカウント値iを起点として所定の範囲内に位置するカウント値（例えばカウント値（i+1），（i+2），……，（i+N））それぞれに鍵で署名して各認証子E（i+1），E（i+2），……，E（i+N）を作成し、今回ユーザから送信されてきた認証子E（j）が、それらの認証子E（i+1），E（i+

2)，……，E(i+N)のうちのいずれかの認証子と一致する場合に，その認証子E(j)の発信元が正しいユーザであると認証し，かつその一致した認証子に対応するカウント値(j)を，次回に認証のために記録するように構成してもよい。この場合，センタは，カウント値自身（本発明にいう第1の符号）を必要としない代わりに，そのカウント値（第1の符号）があらかじめ決めておいた所定の範囲内にあることを期待している。

【0030】さらに，上記の第1実施形態では，図2を参照して説明したように，センタにおいて，認証子は正しい（本発明にいう第2のルールは満足する）ものの，ユーザからのカウント値がセンタに記録されたカウント値よりも小さい（本発明にいう第1のサブルールを満足しない）旨判定された場合に，センタからユーザに向けて乱数を送信し，ユーザからは，その乱数とカウント値（本発明にいう第3の符号）とが結合されてなる結合符号に鍵で署名してなる認証子と，そのカウント値自身（第3の符号）との双方をセンタに送信したが，ユーザからセンタに送信する認証子は乱数のみを鍵で署名してなる認証子であってもよい。その場合であっても，ユーザからセンタにかかるカウント値（第3の符号）を送信する必要がある。乱数のみに鍵で署名してなる認証子をセンタに送信する場合であってもカウント値（第3の符号）も送信するのは，今回の認証のためではなく，次回の認証のためである。

【0031】図3は，本発明の第2実施形態の認証方式におけるデータの流れを示す図である。ここでは，図1を参照して説明した第1実施形態との相違点について説明する。この図3に示す第2実施形態では，図2に示す項目番号2，4，6，7，すなわち，ユーザがセンタ11に向けて認証情報を送信する場合，カウント値に関し項目番号2を例に説明すると，そのときのカウント値(i)と，そのカウント値(i)と送信先のセンタ11を特定するセンタID符号(C1)とを結合してなる結合符号(i，C1)に鍵で署名してなる認証子E(i，C1)との双方からなる認証情報(i，E(i，C1))をセンタ11に向けて送信し，ユーザ10は，その後，カウント値(i)をインクリメントしてカウント値(i+1)とする。

【0032】また，図3に示す項目番号3，5，8では，センタ11は，カウント値に関し項目番号3を例に説明すると，今回送信されてきた認証情報(i，E(i，C1))に含まれるカウント値(i)が前回送信されてきた認証情報(i-1，E(i-1，C1))に含まれていたカウント値(i-1)よりも値の大きなカウント値であるという第1のサブルールと，認証情報(i，E(i，C1))に含まれる認証子E(i，C1)が，その認証情報(i，E(i，C1))に含まれるカウント値(i)と，自分自身のセンタID符号(C1)とを結合してなる結合符号(i，C1)に鍵で署名してなる認証子E(i，C1)と比べ同一の認証子であるという第2のサブルールとの双方のサブルールからなるルールに従うか否かを調べ，そのルールに従っていた場合に，その認証情報(i，E(i，C1))の発信元が正しくユーザ10であることを認証する。またセンタ11は，その認証情報の発信元が正当なユーザ10であるので，そのユーザにサービスを提供する。

【0033】図3に示す項目番号9，10における各処理は，それぞれ，上述した項目番号2，4，6，7における処理，および項目番号3，5，8における処理と比べ，センタID符号がセンタ12を特定するセンタID符号（C2）に変更されるだけであり，重複説明は省略する。この図3に示す第2実施形態では，ユーザ10からセンタ11，12に向けて認証情報を送る場合に，どのセンタ宛に送る認証情報であるかを明記し，その宛先を改ざんされないように，カウント値とその宛先（センタID符号）との双方からなる結合符号に署名する。こうすることにより，ユーザ10がセンタ11に送ろうとしていた認証情報が例えば悪意の第3者によってセンタ12に送られてしまった場合の，誤った認証を防止することができる。

【0034】尚，図3を参照して説明した第2実施形態は，第1実施形態における，カウント値に鍵で署名して認証子を作成することに代え，カウント値とセンタID符号とが結合されてなる結合符号に鍵で署名して認証子を作成するものであり，この点のみ変更すれば，上述した第1実施形態の変形例等がそのまま適用される。したがってここでは第2実施形態についてのこれ以上の説明は省略する。

【0035】図4は，本発明の第3実施形態の認証方式の流れを示す図である。尚，以下に示す項目番号1～8のうち項目番号2～8と同一の番号を図4に付して説明する。

1．前提

図4に示すユーザ30，センタ31，32は，それぞれ，現在時刻を知る時計を有する。またユーザ30は，そのユーザ30の時計による時刻に署名する鍵をセンタ31，32に予め登録しておく。一方，センタ31，32は，ユーザ30の時計による，以前の認証処理によって得られたアクセス時刻を保持する。またセンタ31，32は，センタ31，32それぞれの時計による，そのセンタ31，32へのアクセス時刻を保持する。尚，ユーザ30の時計による，センタ31へのアクセス時刻（tu01）とセンタ32へのアクセス時刻（tu02）は互いに異なる。また，センタ31の時計によるそのセンタ31へのアクセス時刻（tc01）と，センタ32の時計によるそのセンタ32へのアクセス時刻（tc02）も互いに異なる。アクセス時刻tu01とtc01も通常異なる。同様に，アクセス時刻tu02とアクセス時刻tc02も通常異なる。

2．センタ31への認証依頼（その1）
ユーザ30は，認証を受けるにあたり，そのユーザ30の時計（本発明にいう第1の時計）による時刻tu1と，その時刻tu1に鍵で署名してなる認証子E（tu1）との双方からなる認証情報（tu1，E（tu1））をセンタ31に向けて送信する。
3．センタ31での認証処理
センタ31は，今回送信されてきた認証情報（tu1，E（tu1））に含まれる時刻tu1が前回送信されてきた認証情報（tu01，E（tu01））に含まれていた時刻tu01よりも先に進んだ時刻であって，かつ今回送信されてきた認証情報（tu1，E（tu1））に含まれる認証子E（tu1）が，今回送信されてきた認証情報（tu1，E（tu1））に含まれる時刻tu1に鍵で署名してなる認証子と比べ同一の認証子であるというルールに従うか否かを調べ，そのルールに従っていた場合に，さらに，その認証情報（tu1，E（tu1））に含まれる時刻tu1が表わす現在時刻の，前回送信されてきた認証情報（tu01，E（tu01））に含まれる時刻tu01が表わす現在時刻からの第1の経過時間（tu1－tu01）と，センタ31の時計（本発明にいう第2の時計）から得られた，今回送信されてきた認証情報（tu1，E（tu1））の受信時刻tc1の，前回送信されてきた認証情報（tu01，E（tu01））の受信時刻tc01からの第2の経過時間（tc1－tc01）とを比べる。即ち，|（tu1－tu01）－（tc1－tc01）|（ただし，||は絶対値を示す）を計算し，その計算結果が所定の許容誤差（例えば，30秒）以内にある場合に，その認証情報（tu1，E（tu1））の発信元が正しくユーザ30であることを認証する。また，センタ31では，時刻tu1，tc1を記録する。さらに，今回の認証情報の発信元が正当なユーザ30であるので，そのユーザ30にサービスを提供する。
【0036】次に，上述した処理に引き続き認証要求を行った結果，通信に失敗した場合について説明する。
4．センタ31への認証依頼（その2）
ユーザ30は，認証を受けるにあたり，そのユーザ30の時計による時刻tu2と，その時刻tu2に鍵で署名してなる認証子E（tu2）との双方からなる認証情報（tu2，E（tu2））をセンタ31に向けて送信する。しかし，この通信は失敗しセンタ31からの応答がないので，ユーザ30では，その通信処理はタイムアウトと判断し，あらためて認証を依頼する。
5．センタ31への認証依頼（その3）
ユーザ30は，認証を受けるにあたり，そのユーザ30の時計による時刻tu3と，その時刻tu3に鍵で署名してなる認証子E（tu3）との双方からなる認証情報（tu3，E（tu3））をセンタ31に向けて送信する。

6．センタ31での認証処理
センタ31は，今回送信されてきた認証情報（tu3，E（tu3））が前述したルールに従うか否かを調べ，そのルールに従っていた場合に，さらに，その認証情報（tu3，E（tu3））に含まれる時刻tu3が表わす現在時刻の，前回送信されてきた認証情報（tu1，E（tu1））に含まれる時刻tu1が表わす現在時刻からの第1の経過時間（tu3－tu1）と，センタ31の時計から得られた，今回送信されてきた認証情報（tu3，E（tu3））の受信時刻tc3の，前回送信されてきた認証情報（tu1，E（tu1））の受信時刻tc1からの第2の経過時間（tc3－tc1）とを比べる。即ち，|（tu3－tu1）－（tc3－tc1）|（ただし，||は絶対値を示す）を計算し，その計算結果が所定の許容誤差（例えば，30秒）以内にある場合に，その認証情報（tu3，E（tu3））の発信元が正しくユーザ30であることを認証する。また，センタ31では，時刻tu3，tc3を記録する。さらに，その認証情報の発信元が正当なユーザ30であるので，そのユーザ30にサービスを提供する。
【0037】次に，上述した処理に引き続き，センタ31以外のセンタ32に認証要求を行う場合について説明する。
7．センタ32への認証依頼（その1）
ユーザ30は，認証を受けるにあたり，そのユーザ30の時計による時刻tu4と，その時刻tu4に鍵で署名してなる認証子E（tu4）との双方からなる認証情報（tu4，E（tu4））をセンタ32に向けて送信する。
8．センタ32の認証処理
センタ32は，今回送信されてきた認証情報（tu4，E（tu4））が前述したルールに従うか否かを調べ，そのルールに従っていた場合に，さらに，その認証情報（tu4，E（tu4））に含まれる時刻tu4が表わす現在時刻の，前回送信されてきた認証情報（tu02，E（tu02））に含まれる時刻tu02が表わす現在時刻からの第1の経過時間（tu4－tu02）と，センタ32の時計から得られた，今回送信されてきた認証情報（tu4，E（tu4））の受信時刻tc04の，前回送信されてきた認証情報（tu02，E（tu02））の受信時刻tc02からの第2の経過時間（tc4－tc02）とを比べる。即ち|（tu4－tu02）－（tc4－tc02）|（ただし，||は絶対値を示す）を計算し，その計算結果が所定の許容誤差（例えば，30秒）以内にある場合に，その認証情報（tu4，E（tu4））の発信元が正しくユーザ30であることを認証する。また，センタ32では，時刻tu4，tc4を記録する。さらに，その認証情報の発信元が正当なユーザ30であるので，そのユーザ30にサービスを提供する。

【００３８】このように本発明の第３実施形態の認証方式では、ユーザとセンタとの双方に時計を備えているため、ユーザはセンタごとに送った認証子を記録しておく必要がなく、異なるセンタにアクセスする場合でも同じ機構で認証依頼を行なうことができる。また、センタにおける認証は、ユーザの時計がセンタの時計と同じ時間だけ進んでいればよく、ユーザの時計とセンタの時計との間に誤差があってもよい。また、図２に示す、センタがユーザに向けて乱数を送信する手法と組み合わせることにより、安全性をさらに高めることができ、またユーザ側システムの再インストールなどによってユーザの時計がリセットされた場合でも対処できる。

【００３９】尚、図４を参照して説明した第３実施形態において、時刻のみを鍵で署名して認証子を作成することに代え、前述した第２実施形態のように、時刻とセンタＩＤ符号とが結合されてなる結合符号を鍵で署名して認証子を作成してもよい。こうすれば、センタ３１に送信されるべき認証情報がセンタ３２に届いたときの誤った認証を防止することができる。

【００４０】

【発明の効果】以上説明したように、本発明の認証方式によれば、センタにおける認証は、今回送信されてきた第１の認証情報に含まれる第１の符号が前回送信されてきた第２の認証情報に含まれていた符号よりも後に位置する符号であって、かつ、第１の認証情報に含まれる第１の認証子が、その第１の認証情報に含まれる第１の符号（もしくは第１の符号とセンタＩＤ符号とが結合され＊てなる結合符号）に鍵で署名してなる認証子と比べ同一の認証子であるというルールに基づいてなされるため、認証子がセンタに届かない場合であっても、引き続き認証処理を簡単に行うことができる。また、ユーザは送った認証子をセンタごとに記録しておく必要がなく、異なるセンタにアクセスする場合でも同じ機構で認証処理を行うことができる。

【図面の簡単な説明】

【図１】本発明の第１の実施形態の認証方式の流れを示す図である。

【図２】図１に示す認証方式において、センタが認証依頼を受けた場合、ユーザからのカウント値がセンタに記録されたカウント値よりも小さい場合の処理について示した図である。

【図３】本発明の第２実施形態の認証方式の流れを示す図である。

【図４】本発明の第３実施形態の認証方式の流れを示す図である。

【図５】従来のチャレンジ・レスポンス型の認証方式の流れを示す図である。

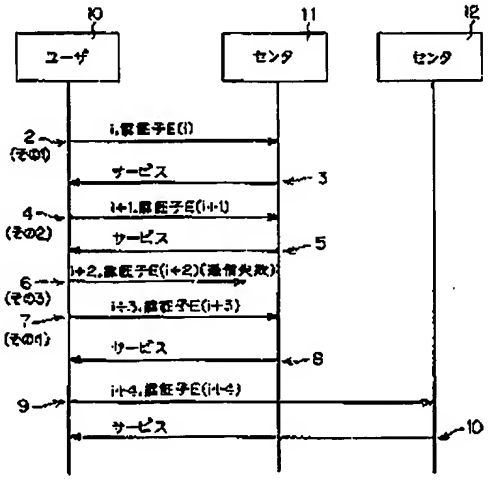
【図６】特開平５－２１９０５３号公報に提案されたチャレンジ・レスポンス型の認証方式の流れを示す図である。

【符号の説明】

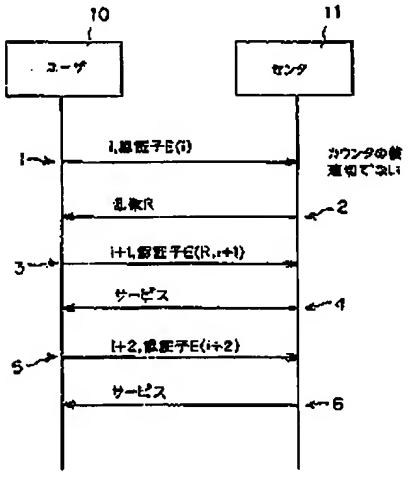
１０，３０　ユーザ

１１，１２，３１，３２　センタ

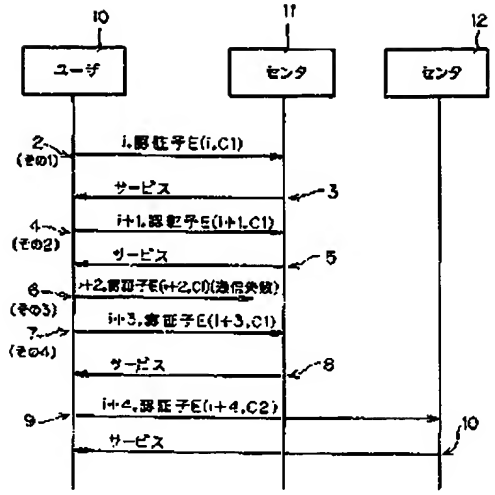
【図１】



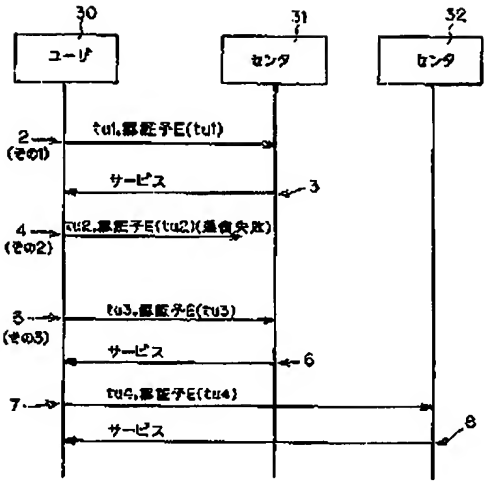
【図２】



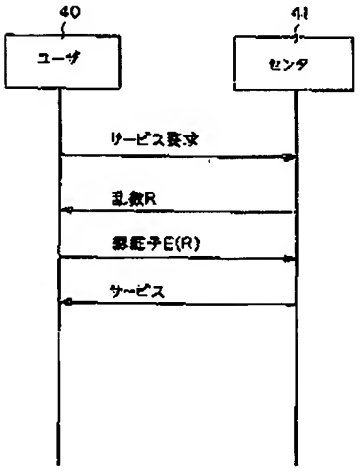
【図3】



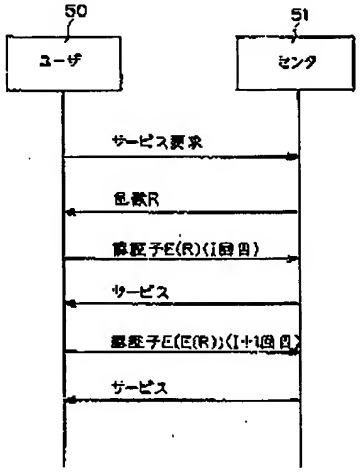
【図4】



【図5】



【図6】



フロントページの続き

(72)発明者　鳥居　直哉
神奈川県川崎市中原区上小田中4丁目1番1号　富士通株式会社内

(72)発明者　武仲　正彦
神奈川県川崎市中原区上小田中4丁目1番1号　富士通株式会社内

[Claim(s)]
[Claim 1] The center which attests that it is the information to which this information has been transmitted from just dispatch origin based on the transmitted information, In the authentication method which performs said authentication between the users who receive authentication of being the information which transmitted information towards this center and was disseminated from dispatch origin with this just information on the both sides of said user and said center The both sides of the information showing the sequence of this sign that constitutes the set of the sign as which sequence was determined, and the key which signs a sign are shared. Said user The sign which it comes to update according to said sequence whenever it is going to receive the authentication which constitutes said set in receiving said authentication, The authentication information which consists of both sides with the authentication child who comes to sign this sign with said key is turned to said center, and it transmits. Said center The 1st subrule that it is the sign in which the 1st sign contained in the 1st authentication information transmitted this time is behind located according to said sequence rather than the 2nd sign contained in the 2nd authentication information transmitted last time from said user, It investigates whether the 1st Ruhr which consists of a subrule of both sides with the 2nd subrule that he is the same authentication child compared with the authentication child who comes to sign the 1st sign contained in the 1st authentication information with said key is followed. the 1st authentication child contained in the 1st authentication information -- this -- the case where this 1st Ruhr is followed -- this -- the authentication method characterized by attesting that the dispatch origin of the 1st authentication information is said user surely.
[Claim 2] The center which attests that it is the information to which this information has been transmitted from just dispatch origin based on the transmitted information, In the authentication method which performs said authentication between the users who receive authentication of being the information which transmitted information towards this center and was disseminated from dispatch origin with this just information on the both sides of said user and said center The both sides of the information showing the sequence of this sign that constitutes the set of the sign as which sequence was determined, and the key which signs a sign are shared. Said user The sign which it comes to update according to said sequence whenever it is going to receive the authentication which constitutes said set in receiving said authentication, Turn to said center the authentication information which consists of both sides with the authentication child who comes to sign the joint sign which comes to join together this sign and the center ID code which specifies the center of a transmission place with said key, and it transmits. The 1st subrule that said center is a sign in which the 1st sign contained in the 1st authentication information

transmitted this time is behind located according to said sequence rather than the 2nd sign contained in the 2nd authentication information transmitted last time from said user, The 1st authentication child contained in the 1st authentication information It investigates whether the 1st Ruhr which consists of a subrule of both sides with the 2nd subrule that he is the same authentication child compared with the authentication child who comes to sign the joint sign which comes to join together the 1st sign and its own center ID code which are contained in the 1st authentication information with said key is followed. this -- the case where this 1st Ruhr is followed -- this -- the authentication method characterized by attesting that the dispatch origin of the 1st authentication information is said user surely.

[Claim 3] Said center is an authentication method according to claim 1 or 2 characterized by adopting the subrule to which the regulation of being the sign to which said 1st sign is located within the limits of predetermined according to said sequence with said 2nd sign as the starting point was added as said 1st subrule.

[Claim 4] Said center is an authentication method according to claim 1 or 2 characterized by judging with it being an authentication demand unjust when the 1st authentication information transmitted this time does not follow said 2nd subrule.

[Claim 5] Although the 1st authentication information transmitted this time needs said center for said 2nd subrule therefore, when said 1st subrule is not followed The random number generated in this center is transmitted to said user. Said user From said center, the 3rd authentication information including the 2nd authentication child who comes to sign the transmitted random number with said key is turned to said center, and it transmits. Said center It investigates whether the 2nd Ruhr that he is the same authentication child compared with the authentication child who comes to sign said random number which the 2nd authentication child contained in the 3rd authentication information transmitted this time generated in this center with said key is followed. The authentication method according to claim 1 or 2 with which both sides with 3rd authentication information transmitted 1st authentication information [which has been transmitted last time] and this time when this 2nd Ruhr is followed dispatch-origin is characterized by attesting that he is said user surely.

[Claim 6] The authentication method according to claim 5 characterized by being a thing containing the 3rd sign said whose 3rd authentication information is the sign of either of the signs which constitute said set.

[Claim 7] Said user is what transmits the authentication child who comes to sign the joint sign with which it comes to combine said random number and said 3rd sign with said key as said 2nd authentication child to said center. Said center as said 2nd Ruhr The 2nd authentication child contained in the 3rd authentication information transmitted this time The authentication method according to claim 6 characterized by being what adopts the Ruhr that he is the same authentication child compared with the authentication child who comes to sign the joint sign with which it comes to combine said random number generated in this center, and the 3rd sign contained in the authentication information transmitted this time with said key.

[Claim 8] The center which attests that it is the information to which this information has been transmitted from just dispatch origin based on the transmitted information, In the authentication method which performs said authentication between the users who receive authentication of being the information which transmitted information towards this center and was disseminated from dispatch origin with this just information on the both sides of said user and said center The both sides of the information showing the sequence of this sign that constitutes the set of the sign as which sequence was determined, and the key which signs a sign are shared. Said user Turn to

said center authentication information including the authentication child who comes to sign the sign which it comes to update according to said sequence whenever it is going to receive the authentication which constitutes said set in receiving said authentication with said key, and it transmits. The 1st authentication child contained in the 1st authentication information transmitted this time said center It is the sign behind located according to said sequence rather than the 2nd sign contained in the 2nd authentication information transmitted last time from said user. And when the 1st Ruhr that he is the same authentication child as the authentication child of either of each authentication child who comes to sign each sign located within the limits of predetermined according to said sequence with this 2nd sign as the starting point with said key is followed this -- the authentication method characterized by attesting that the dispatch origin of the 1st authentication information is said user surely.

[Claim 9] The center which attests that it is the information to which this information has been transmitted from just dispatch origin based on the transmitted information, In the authentication method which performs said authentication between the users who receive authentication of being the information which transmitted information towards this center and was disseminated from dispatch origin with this just information on the both sides of said user and said center The both sides of the information showing the sequence of this sign that constitutes the set of the sign as which sequence was determined, and the key which signs a sign are shared. Said user Turn to said center authentication information including the authentication child who comes to sign the joint sign which comes to join together the sign which it comes to update according to said sequence whenever it is going to receive the authentication which constitutes said set in receiving said authentication, and the center ID code which specifies the center of a transmission place with said key, and it transmits. The 1st authentication child contained in the 1st authentication information transmitted this time said center It is the sign behind located according to said sequence rather than the 2nd sign contained in the 2nd authentication information transmitted last time from said user. and When the 1st Ruhr that he is the same authentication child as the authentication child of either of each authentication child who comes to sign each joint sign which comes to join together each sign and its own center ID code which are located within the limits of predetermined according to said sequence with this 2nd sign as the starting point with said key is followed this -- the authentication method characterized by attesting that the dispatch origin of the 1st authentication information is said user surely.

[Claim 10] It is the authentication method according to claim 1 or 7 which said user has the 1st clock which gets to know current time, and is characterized by this user being a thing using the sign showing the current time obtained from this clock as a sign which constitutes said set.

[Claim 11] Said center has the 2nd clock which gets to know current time. This center While the 1st authentication information transmitted this time follows said 1st Ruhr furthermore -- this -- the current time which the 1st sign contained in the 1st authentication information expresses The 1st elapsed time from current time which the 2nd sign contained in the 2nd authentication information transmitted last time expresses The receipt time of the 1st authentication information which was acquired from said 2nd clock and which has been transmitted this time, the case where it is within a predetermined allowable error compared with the 2nd elapsed time from the receipt time of the 2nd authentication information transmitted last time -- this -- the authentication method according to claim 10 characterized by attesting that the dispatch origin of the 1st authentication information is said user surely.

[Detailed Description of the Invention]

[0001]
[Field of the Invention] This invention relates to the authentication method which performs authentication between the center which attests that it is the information to which the information has been transmitted from just dispatch origin based on the transmitted information, and the user who receives authentication of being the information which transmitted information towards the center and was disseminated from dispatch origin with the just information.
[0002]
[Description of the Prior Art] Before, the authentication method of the following types (mold) is learned as above authentication methods.
1) The authentication method user of a password mold registers the password into the center beforehand, in receiving authentication, turns the password to a center and transmits. In the center, when in agreement with the password with which the transmitted password is registered beforehand, it attests that the password dispatch-origin is a right user. This method results in allowing unjust access to the center by that holder in bad faith, when that password is intercepted by the holder in bad faith.
2) On the both sides of a consecutive-numbers type authentication method user and a center, it has a counter (this counter may use time of day that what is necessary is just the thing of the increment sequence of numbers in monotone), and in receiving authentication, a user turns the value of the counter by the side of a user to a center, and transmits. In the center, when the value of the transmitted counter and the value of the counter by the side of a center are in agreement, it attests that the dispatch origin of the value of the counter is a right user. By this method, when the value thru/or time of day of a counter needs to be completely in agreement in the user and the center, the user was going to access the center and it failed, or when two or more centers are accessed, there is a possibility that the values of a counter may differ and time of day is adopted, a user's clock and the clock of a center need to be completely in agreement. Moreover, the value of the transmitted counter is intercepted and it results in allowing unjust access by generating the value of the following counter immediately and transmitting etc.
3) consecutive numbers -- it has a counter to the both sides of the authentication method user of a signature mold, and a center. Moreover, a user registers the key into the center beforehand while having the key which enciphers the value of a counter. In receiving authentication, a user creates a signature (authentication child) for the value of the counter by the side of a user with the key, turns the signature to a center and transmits. On the other hand, in the center, when the signature (authentication child) which signed with the key registered into the value of the counter by the side of a center, and was created, and the signature transmitted by the user are in agreement, it attests that the dispatch origin of the signature is a right user. Here, whenever the value of the counter by the side of a user and the value of the counter by the side of a center attest, the increment of them is carried out. Although safety increases considerably at that point since in the case of this method the value of a counter is not known even if intercepted, problems -- it is necessary to make the value of a counter always in agreement etc. -- remain.
4) Authentication method drawing 5 of a challenge response mold is drawing showing the flow of the authentication method of the conventional challenge response mold.
[0003] The user 40 who shows drawing 5 registers the key into the center 41 while having the key which signs a random number R. First, a user 40 turns a service request to a center 41, and transmits. Then, in attesting in response to this service request, a center 41 transmits a random number R towards a user 40. A user 40 signs the transmitted random number R with the key which the user 40 has, creates authentication child E (R) and (a signature of a random number

R), turns authentication child E (R) to a center 41, and transmits. It signs with the key registered into the random number R also in the center 41 on the other hand, and when authentication child E (R) transmitted by the user 40 is in agreement with the authentication child who created and created the authentication child, it attests that the dispatch origin of authentication child E (R) is the right user 40, and the user 40 is provided with service. In the case of this method, since the random number which cannot be predicted is signed with a key, the safety to a holder in bad faith is raised further.

[0004] prediction of the message transmitted by four kinds of authentication methods mentioned above for authentication -- a password mold and consecutive numbers -- a mold and consecutive numbers -- it becomes difficult in order of a signature mold and a challenge response mold. for this reason, the safety to unjust access to the center by the inaccurate user -- a password mold and consecutive numbers -- a mold and consecutive numbers -- it rises in order of a signature mold and a challenge response mold. For this reason, many authentication methods of a challenge response mold are used conventionally.

[0005] on the other hand -- authentication processing -- a password mold and consecutive numbers -- a mold and consecutive numbers -- it becomes more complicated and more complicated in order of a signature mold and a challenge response mold. For this reason, when many times authentication processing was continuously needed, the demand which simplifies authentication processing came out, securing safety comparable as the authentication method of a challenge response mold. In order to fill this demand, JP,5-219053,A has one proposal.

[0006] Drawing 6 is drawing showing the flow of the authentication method of the challenge response mold proposed by JP,5-219053,A. In carrying out by repeating authentication processing, by this authentication method, the authentication child (E (R)) whom the user 50 created to the Ith time on a user 50 and the both sides of a center 51 is used as I+1st random-numbers E (R). For this reason, when repeating simple authentication processing of the authentication method of the challenge response mold which it is not necessary to send a random number to the I+1st time, and processing of that whole part ends quickly, and is shown in drawing 4 mentioned above, even if it compares a center 51, safety does not fall.

[0007]

[Problem(s) to be Solved by the Invention] However, when it carries out using the authentication method of the challenge response mold using the authentication child who created to the Ith time as the I+1st random numbers mentioned above by repeating authentication processing using a communication line without the guarantee in which an authentication child like the Internet not necessarily reaches a center, an authentication child may fail in turbulence and authentication.

[0008] Moreover, if this authentication method is used for the service which accesses two or more centers at random like WWW (World Wide Web), a user needs to record the authentication child who transmitted for every center, and, for this reason, the device by the side of a user will become complicated. This invention aims at offering the authentication method which can perform authentication processing easily after securing sufficient safety in view of the above-mentioned situation.

[0009]

[Means for Solving the Problem] The 1st authentication method of the authentication methods of this invention which attains the above-mentioned purpose The center which attests that it is the information to which the information has been transmitted from just dispatch origin based on the transmitted information, In the authentication method which performs the above-mentioned authentication between the users who receive authentication of being the information which

transmitted information towards the center and was disseminated from dispatch origin with the just information on the both sides of the above-mentioned user and the above-mentioned center The both sides of the information showing the sequence of those signs that constitute the set of the sign as which sequence was determined, and the key which signs a sign are shared. The above-mentioned user The sign which it comes to update according to the above-mentioned sequence whenever it is going to receive the authentication which constitutes the above-mentioned set in receiving the above-mentioned authentication, The authentication information which consists of both sides with the authentication child who comes to sign the sign with the above-mentioned key is turned to the above-mentioned center, and it transmits. The above-mentioned center The 1st subrule that it is the sign in which the 1st sign contained in the 1st authentication information transmitted this time is behind located according to the above-mentioned sequence rather than the 2nd sign contained in the 2nd authentication information transmitted last time from the user, It investigates whether the 1st Ruhr which consists of a subrule of both sides with the 2nd subrule that he is the same authentication child compared with the authentication child to whom the 1st authentication child contained in the 1st authentication information comes to sign the 1st sign contained in the 1st authentication information with the above-mentioned key is followed. When the 1st Ruhr is followed, the dispatch origin of the 1st authentication information is characterized by attesting that he is the above-mentioned user surely.

[0010] Moreover, the 2nd authentication method of this invention which attains the above-mentioned purpose The center which attests that it is the information to which the information has been transmitted from just dispatch origin based on the transmitted information, In the authentication method which performs the above-mentioned authentication between the users who receive authentication of being the information which transmitted information towards the center and was disseminated from dispatch origin with the just information on the both sides of the above-mentioned user and the above-mentioned center The both sides of the information showing the sequence of those signs that constitute the set of the sign as which sequence was determined, and the key which signs a sign are shared. The above-mentioned user The sign which it comes to update according to the above-mentioned sequence whenever it is going to receive the authentication which constitutes the above-mentioned set in receiving the above-mentioned authentication, Turn to the above-mentioned center the authentication information which consists of both sides with the authentication child who comes to sign the joint sign which comes to join together the sign and the center ID code which specifies the center of a transmission place with the above-mentioned key, and it transmits. The 1st subrule that the above-mentioned center is a sign in which the 1st sign contained in the 1st authentication information transmitted this time is behind located according to the above-mentioned sequence rather than the 2nd sign contained in the 2nd authentication information transmitted last time from the user, The 1st authentication child contained in the 1st authentication information It investigates whether the 1st Ruhr which consists of a subrule of both sides with the 2nd subrule that he is the same authentication child compared with the authentication child who comes to sign the joint sign which comes to join together the 1st sign and its own center ID code which are contained in the 1st authentication information with the above-mentioned key is followed. When the 1st Ruhr is followed, the dispatch origin of the 1st authentication information is characterized by attesting that he is the above-mentioned user surely.

[0011] Here, as for the above-mentioned center, in the 1st authentication method of above-mentioned this invention thru/or the 2nd authentication method, it is desirable to adopt the

subrule to which the regulation of being the sign to which the 1st sign of the above is located within the limits of predetermined according to the above-mentioned sequence with the 2nd sign as the starting point of the above was added as a subrule of the above 1st. Moreover, in the above-mentioned center, when the 1st authentication information transmitted this time does not follow the subrule of the above 2nd, it is judged with it being an unjust authentication demand.

[0012] In the 1st authentication method of above-mentioned this invention, and the 2nd authentication method moreover, the above-mentioned center Although the 1st authentication information transmitted this time is needed for the subrule of the above 2nd therefore, when the subrule of the above 1st is not followed The random number generated in the center is transmitted to the above-mentioned user. The above-mentioned user From the above-mentioned center, the 3rd authentication information including the 2nd authentication child who comes to sign the transmitted random number with the above-mentioned key is turned to the above-mentioned center, and it transmits. The above-mentioned center It investigates whether the 2nd Ruhr that he is the same authentication child compared with the authentication child who comes to sign the above-mentioned random number which the 2nd authentication child contained in the 3rd authentication information transmitted this time generated in the center with the above-mentioned key is followed. When this 2nd Ruhr is followed, it is effective to attest that both sides with 3rd authentication information transmitted 1st authentication information [which has been transmitted last time] and this time dispatch-origin is the above-mentioned user surely.

[0013] It is desirable that it is a thing containing the 3rd sign whose authentication information on the above 3rd is the sign of either of the signs which constitute the above-mentioned set. Further in that case in this case, the above-mentioned user It is what transmits the authentication child who comes to sign the joint sign with which it comes to combine the above-mentioned random number and the 3rd sign of the above with the above-mentioned key as an authentication child of the above 2nd to the above-mentioned center. The above-mentioned center The 2nd authentication child contained in the 3rd authentication information transmitted this time as the 2nd Ruhr of the above It is desirable that it is what adopts the Ruhr that he is the same authentication child compared with the authentication child who comes to sign the joint sign with which it comes to combine the above-mentioned random number generated in the center and the 3rd sign contained in the authentication information transmitted this time with the above-mentioned key.

[0014] Moreover, the 3rd authentication method of the authentication methods of this invention which attains the above-mentioned purpose The center which attests that it is the information to which the information has been transmitted from just dispatch origin based on the transmitted information, In the authentication method which performs the above-mentioned authentication between the users who receive authentication of being the information which transmitted information towards the center and was disseminated from dispatch origin with the just information on the both sides of the above-mentioned user and the above-mentioned center The both sides of the information showing the sequence of those signs that constitute the set of the sign as which sequence was determined, and the key which signs a sign are shared. The above-mentioned user Turn to the above-mentioned center authentication information including the authentication child who comes to sign the sign which it comes to update according to the above-mentioned sequence whenever it is going to receive the authentication which constitutes the above-mentioned set in receiving the above-mentioned authentication with the above-mentioned key, and it transmits. The 1st authentication child contained in the 1st authentication information transmitted this time the above-mentioned center It is the sign behind located according to the

above-mentioned sequence rather than the 2nd sign contained in the 2nd authentication information transmitted last time from the user. And when the 1st Ruhr that he is the same authentication child as the authentication child of either of each authentication child who comes to sign each sign located within the limits of predetermined according to the above-mentioned sequence with the 2nd sign as the starting point with the above-mentioned key is followed The dispatch origin of the 1st authentication information is characterized by attesting that he is the above-mentioned user surely.

[0015] Furthermore, the 4th authentication method of the authentication methods of this invention The center which attests that it is the information to which the information has been transmitted from just dispatch origin based on the transmitted information, In the authentication method which performs the above-mentioned authentication between the users who receive authentication of being the information which transmitted information towards the center and was disseminated from dispatch origin with the just information on the both sides of the above-mentioned user and the above-mentioned center The both sides of the information showing the sequence of those signs that constitute the set of the sign as which sequence was determined, and the key which signs a sign are shared. The above-mentioned user Turn the authentication information included in the authentication child who comes to sign the joint sign which comes to join together the sign which it comes to update according to the above-mentioned sequence whenever it is going to receive the authentication which constitutes the above-mentioned set in receiving the above-mentioned authentication, and the center ID code which specifies the center of a transmission place with said key to the above-mentioned center, and it transmits. The 1st authentication child contained in the 1st authentication information transmitted this time the above-mentioned center It is the sign behind located according to the above-mentioned sequence rather than the 2nd sign contained in the 2nd authentication information transmitted last time from the user. and When the 1st Ruhr that he is the same authentication child as the authentication child of either of each authentication child who comes to sign each joint sign which comes to join together each sign and its own center ID code which are located within the limits of predetermined according to the above-mentioned sequence with the 2nd sign as the starting point with the above-mentioned key is followed The dispatch origin of the 1st authentication information is characterized by attesting that he is the above-mentioned user surely.

[0016] here -- the 1- of above-mentioned this invention -- in the 4th authentication method, the above-mentioned user has the 1st clock which gets to know current time, and the user may use the sign showing the current time obtained from the clock as a sign which constitutes the above-mentioned set. The above-mentioned center has further the 2nd clock which gets to know current time. In that case, the center While the 1st authentication information transmitted this time follows the 1st Ruhr of the above Furthermore, the current time which the 1st sign contained in the 1st authentication information expresses, The 1st elapsed time from current time which the 2nd sign contained in the 2nd authentication information transmitted last time expresses The receipt time of the 1st authentication information which was acquired from the 2nd clock of the above and which has been transmitted this time, When it is within a predetermined allowable error compared with the 2nd elapsed time from the receipt time of the 2nd authentication information transmitted last time, it is desirable to attest that the dispatch origin of the 1st authentication information is the above-mentioned user surely.

[0017]

[Embodiment of the Invention] Hereafter, the operation gestalt of this invention is explained. Drawing 1 is drawing showing the data flow in the authentication method of the 1st operation gestalt of this invention. In addition, in order to give explanation easy here, the same number as the item numbers 2-10 indicated below is given to the arrow head which shows the data flow of drawing 1 , and is explained.

1. Premise (this Number 1 is not Entered in Drawing 1)

The user 10 who shows drawing 1 has the both sides of a counter and the key which signs the counted value of the counter. The counted value of this counter is equivalent to the sign said to this invention, and a series of counted value of that counter is equivalent to the set of the sign said to this invention. Here, suppose that the current counted value of this counter is counted value (i). Moreover, the user 10 registers into two centers 11 and 12 the key which signs counted value. On the other hand, centers 11 and 12 hold the counted value obtained by former authentication processing of a user 10 (here, the counted value of a center 11 is the counted value (i-2) of (i-1) and a center 12, and such counted value differs mutually). Thus, the both sides of a user 10 and centers 11 and 12 are sharing both sides with the information (information showing the sequence of the sign said to this invention), i.e., the information that the sequential increment of the counted value is carried out, that the counter used here is a rise counter, and the key for signing counted value here.

2. Authentication Request to Center 11 (the 1)

In receiving authentication, a user 10 turns to a center 11 the authentication information (i, E (i)) which consists of counted value at that time (i), and both sides with authentication child E (i) which comes to sign the counted value (i) with a key, and transmits. After that, a user 10 increments counted value (i) and is taken as counted value (i+1).

3. Authentication Processing Center 11 in Center 11 The authentication information transmitted this time () [i,] [E] (i) The counted value contained in (the 1st authentication information said to this invention) The 1st subrule that it is counted value with a bigger value than the counted value (i-1) (the 2nd sign said to this invention) contained in the authentication information (i-1, E (i-1)) (2nd authentication information said to this invention) to which (i) and the (1st sign said to this invention) have been transmitted last time, Authentication child E (i) contained in authentication information (i, E (i)) It investigates whether the Ruhr (the 1st Ruhr said to this invention) which consists of a subrule of both sides with the 2nd subrule that he is the same authentication child compared with authentication child E (i) which comes to sign with a key the counted value (i) contained in the authentication information (i, E (i)) is followed. When the Ruhr is followed, the dispatch origin of the authentication information (i, E (i)) attests that he is a user 10 surely. Moreover, a center 11 records the counted value (i) received from the user 10. Furthermore, since the dispatch origin of the authentication information is a valid user 10, a center 11 provides the user 10 with service.

4. Authentication Request to Center 11 (the 2)

In receiving the next authentication, a user 10 turns to a center 11 the authentication information (i+1, E (i+1)) which consists of both sides with the authentication child E (i+1) who comes to sign counted value (i+1) and its counted value (i+1) with a key, and transmits. When it contrasts with this invention, it is equivalent to the 1st authentication information that this authentication information (i+1, E (i+1)) is also said to this invention. A user 10 increments counted value (i+1) after that, and is taken as counted value (i+2).

5. Authentication Processing Center 11 in Center 11 The 1st subrule that it is counted value with a big value from the counted value (i) contained in the authentication information (i, E (i)) to

which the counted value (i+1) contained in the authentication information (i+1, E (i+1)) transmitted this time has been transmitted last time, The authentication child E (i+1) contained in authentication information (i+1, E (i+1)) It investigates whether the Ruhr (the 1st Ruhr said to this invention) which consists of a subrule of both sides with the 2nd subrule that he is the same authentication child compared with the authentication child E (i+1) who comes to sign with a key the counted value (i+1) contained in the authentication information (i+1, E (i+1)) is followed. When the Ruhr is followed, the dispatch origin of the authentication information (i+1, E (i+1)) attests that he is a user 10 surely. Moreover, a center 11 records the counted value (i+1) from a user 10. Furthermore, since the dispatch origin of the authentication information is a valid user 10, a center 11 provides the user 10 with service.

[0018] Although two authentication processings were performed even here, if challenge-response authentication is repeated twice simply, by the authentication method of this operation gestalt, it has ended with four communication links the place for which a communication link on the need of sending a random number to a user 10 from a center 11 is needed 8 times. Next, as a result of continuing at the processing mentioned above and performing an authentication demand, the case where a communication link goes wrong is explained.

6. Authentication Request to Center 11 (the 3)

In receiving authentication, a user 10 turns to a center 11 the authentication information (i+2, E (i+2)) which consists of both sides with the authentication child E (i+2) who comes to sign counted value (i+2) and its counted value (i+2) with a key, and transmits. A user 10 increments counted value (i+2) after that, and is taken as counted value (i+3). However, since this communication link goes wrong and there is no response from a center 11, a user's communications processing serves as a time-out, and requests authentication anew.

7. Authentication Request to Center 11 (the 4)

In receiving authentication, a user 10 turns to a center 11 the authentication information (i+3, E (i+3)) which consists of both sides with the authentication child E (i+3) who comes to sign counted value (i+3) and its counted value (i+3) with a key, and transmits. In addition, it is equivalent to the 1st authentication information that this authentication information (i+3, E (i+3)) is also said to this invention. A user 10 increments counted value (i+3) after that, and is taken as counted value (i+4).

8. Authentication Processing Center 11 in Center 11 The 1st subrule that it is counted value with a bigger value than the counted value (i+1) contained in the authentication information (i+1, E (i+1)) to which the counted value (i+3) contained in the authentication information (i+3, E (i+3)) transmitted this time has been transmitted last time, The authentication child E (i+3) contained in authentication information (i+3, E (i+3)) It investigates whether the Ruhr which consists of a subrule of both sides with the 2nd subrule that he is the same authentication child compared with the authentication child E (i+3) who comes to sign with a key the counted value (i+3) contained in the authentication information (i+3, E (i+3)) is followed. When the Ruhr is followed, the dispatch origin of the authentication information (i+3, E (i+3)) attests that he is a user 10 surely. Moreover, as for a center 11, the dispatch origin of the authentication information records the counted value (i+3) from a user 10. Furthermore, since the dispatch origin of the authentication information is a valid user 10, a center 11 provides the user 10 with service.

[0019] Thus, even if it is the case where authentication information (i+2, E (i+2)) does not arrive at a center 11 The counted value (i+3) contained in the following authentication information (i+3, E (i+3)) in a center 11 is larger than the counted value (i+1) currently recorded on the center 11. And since the authentication child (E (i+3)) contained in authentication information

(i+3, E (i+3)) is also the same authentication child as the authentication child who comes to sign counted value (i+3) with a key, he has succeeded in authentication.
[0020] Next, the case where an authentication demand is given to the center 12 which is a center which is different in a center 11 following on the processing mentioned above is explained.
9. In receiving authentication, the authentication request user 10 to a center 12 turns to a center 12 the authentication information (i+4, E (i+4)) (it is the 1st authentication information that this authentication information is also said to this invention) which consists of both sides with the authentication child E (i+4) who comes to sign counted value (i+4) and its counted value with a key, and transmits. A user 10 increments counted value (i+4) after that, and is taken as counted value (i+5).
10. Authentication Processing Center 12 in Center 12 The 1st subrule that it is counted value with a bigger value than the counted value (i-2) contained in the authentication information (i-2, E (i-2)) to which the counted value (i+4) contained in the authentication information (i+4, E (i+4)) transmitted this time has been transmitted last time, The authentication child E (i+4) contained in authentication information (i+4, E (i+4)) It investigates whether the Ruhr (the 1st Ruhr said to this invention) which consists of a subrule of both sides with the 2nd subrule that he is the same authentication child compared with the authentication child (E (i+4)) who comes to sign with a key the counted value (i+4) contained in the authentication information (i+4, E (i+4)) is followed. When the Ruhr is followed, the dispatch origin of the authentication information (i+4, E (i+4)) attests that he is a user 10 surely. Moreover, a center 12 records the counted value (i+4) from a user 10. Furthermore, since the dispatch origin of the authentication information is a valid user 10, a center 12 provides the user 10 with service.
[0021] Thus, even if a user is the case where it is not necessary to change an authentication child for every center, and which center is accessed, he is good at the same processing, and for this reason, the device by the side of a user becomes easy. In the authentication method shown in drawing 1 , drawing 2 is drawing having shown the processing in the case of being smaller than the counted value by which the counted value from a user was recorded on the center, when a center receives an authentication request.
[0022] A center 11 is judged to be unjust access when an authentication child is not right (when not satisfying the 2nd subrule said to this invention). On the other hand, since the user 10 has reset the counter by a certain reason when an authentication child has the right smaller than the counted value by which the counted value from a user was recorded on the center (the 1st subrule said to this invention is not satisfied), the present counted value is asked to a user 10. The inquiry procedure is explained with reference to drawing 2 . The same number as the item numbers 1-4 indicated below is given to drawing 2 , and is shown.
[0023] 1. In receiving authentication, the authentication request user 10 to a center 11 turns to a center 11 the authentication information (i, Ei) (1st authentication information said to this invention) which consists of both sides with authentication child E (i) which comes to sign the value (i) and the value of a counter of a counter (i) with a key, and transmits. A user 10 increments (i) of a count after that, and makes it counted value (i+1).
[0024] 2. In Authentication Processing Center 11 in Center 11 Since the counted value (i) contained in the authentication information (i, E (i)) transmitted this time is smaller than the counted value (the counted value recorded on the center 11 here presupposes that it was the counted value of a larger value than counted value (i)) recorded on the center 11 Next, when the counted value (i) contained in authentication information (i, E (i)) is signed with a key, an authentication child is created and the created authentication child is not in agreement with

authentication child [from a user 10] E (i), it judges that it is unjust access and a communication link is ended. On the other hand, when the created authentication child is in agreement with authentication child [from a user 10] E (i), a center 11 transmits the random number R which arbitration was made to generate with the random number generator (not shown) with which the center 11 was equipped to a user 10. Moreover, this counted value (i) is recorded temporarily, holding the counted value (i-1) recorded on the center 11 at this time.

[0025] 3. The random number R with which a user's 10 response user 10 has been transmitted from a center 11 It updates from the counted value (i) contained in the authentication information (i, E (i)) which the user 10 transmitted last time. With the authentication child E who comes to sign the joint sign with which it comes to combine the becoming counted value (i+1) (the 3rd sign said to this invention) with a key (R, i+1) (an example of the 2nd authentication child who says this invention) The authentication information (i+1, E (R, i+1)) (3rd authentication information said to this invention) which consists of both sides with the counted value (i+1) is turned to a center 11, and it transmits.

[0026] 4. Authentication Processing Center 11 in Center 11 is Counted Value with Big Value from Counted Value (I) Contained in Authentication Information (I, E (I)) to which Counted Value (I+1) Contained in Authentication Information (I+1, E (R, I+1)) Transmitted this Time Has been Transmitted Last Time. And the random number R which the authentication child E (R, i+1) contained in the authentication information (i+1, E (R, i+1)) transmitted this time generated in the center 11 It investigates whether the Ruhr (an example of the 2nd Ruhr said to this invention) that he is the same authentication child compared with the authentication child who comes to sign with a key the joint sign with which it comes to combine the counted value (i+1) contained in the authentication information (i+1, E (R, i+1)) transmitted this time is followed. When the Ruhr is followed, both sides with authentication information (i+1, E (R, i+1)) transmitted authentication information [which has been transmitted last time] (i, E (i)) and this time dispatch-origin attests that he is a user 10 surely, and offers service. Moreover, the counted value (i+1) sent by the user 10 at this time is recorded. In addition, when the Ruhr is not followed, it is judged as unjust access, and the counted value (i) recorded temporarily is canceled, and it returns to the counted value (i-1) currently recorded before that.

[0027] If it furthermore continues and the authentication request (number 5 shown in drawing 2) to the center 11 by the user 10 is performed, authentication processing (number 6 shown in drawing 2 R> 2) to the authentication request by the center 11 will be performed. Thus, according to the authentication method of the above-mentioned 1st operation gestalt, the authentication in a center is made based on larger counted value than a user's counted value obtained as a result of the authentication in which it succeeded [last]. In other words, it is not necessary to necessarily attest by the authentication child generated from the continuous counted value according to this operation gestalt, and since it is an authentication (that user has key also attests to coincidence, of course) method which attests that counted value is progressing, even if this operation gestalt does not have the guarantee in which an authentication child surely reaches a center, it can carry out authentication processing without excessive processing succeedingly.

[0028] moreover, counted value -- even progressing -- since what is necessary is just to be, a user does not need to record the authentication child who transmitted for every center, and even when accessing a different center, he can perform an authentication request by the same device. Furthermore, with the above-mentioned operation gestalt, since it has the device in which the synchronization of a counter is taken as explained with reference to drawing 2 , in order to raise

safety, also when the value of a user's counter is changed by the case where a user's counted value is changed, re-install of a user side system, etc., it can be coped with easily.

[0029] In addition, the authentication information transmitted as 1st subrule with the operation gestalt of the above 1st this time (For example, authentication information to which the counted value (j) contained in authentication information (j, E (j)) has been transmitted last time (for example, although the subrule that it was counted value (j>i) with a big value was adopted from the counted value (i) contained in authentication information (i, E (i)))) The regulation that |j-i| is in the predetermined range (|j-i|<=n) may be added to this 1st subrule. By carrying out like this, communicative safety is raised further. Moreover, although the both sides of counted value (for example, counted value (j)) and the authentication child (for example, E (j)) who comes to sign the counted value (j) with a key are included in the authentication information transmitted to a center from a user with the 1st above-mentioned operation gestalt The ** which the counted value (for example, counted value (j)) itself does not transmit towards a center as a modification of this 1st operation gestalt from a user, Only the authentication child (for example, E (j)) is transmitted. In the center the counted value (for example, counted value (i+1) --) located within the limits of predetermined with counted value i as the starting point memorized from the user corresponding to the authentication child (for example, E (i)) transmitted last time (i+2), ..., (i+N) -- each -- a key -- signing -- each authentication child E (i+1) -- Authentication child E (j) which created E (i+2), ..., E (i+N), and has been transmitted by the user this time When in agreement with the authentication child of either of those authentication children E (i+1), E (i+2), ..., E (i+N) You may constitute so that it may attest with the dispatch origin of authentication child E (j) being a right user and the counted value (j) corresponding to the authentication child who was in agreement may be recorded for authentication at next time. In this case, the center expects instead of [which does not need the counted value (the 1st sign said to this invention) itself] to be within the limits of predetermined [which that counted value (the 1st sign) determined beforehand].

[0030] Furthermore, with the above-mentioned 1st operation gestalt, as explained with reference to drawing 2 In a center an authentication child A right (the 2nd Ruhr said to this invention is satisfied) thing, When [with the counted value smaller (the 1st subrule said to this invention is not satisfied) than the counted value recorded on the center from a user] a purport judging is carried out Although the random number was transmitted towards the user from the center and the authentication child who comes to sign with a key the joint sign with which it comes to combine from a user the random number and counted value (3rd sign said to this invention), and both sides of counted value own [the] (the 3rd sign) were transmitted to the center The authentication child who transmits to a center from a user may be an authentication child who comes to sign with a key only in a random number. Even if it is that case, it is necessary to transmit the counted value (the 3rd sign) which starts a center from a user. Even if it is the case where the authentication child who comes to sign only a random number with a key is transmitted to a center, counted value (the 3rd sign) does not transmit, either, because [of this authentication], and it is for next authentication.

[0031] Drawing 3 is drawing showing the data flow in the authentication method of the 2nd operation gestalt of this invention. Here, difference with the 1st operation gestalt explained with reference to drawing 1 is explained. If an item number 2 is explained to an example about counted value when the item numbers 2, 4, 6, and 7 shown in drawing 2 , i.e., a user, transmit authentication information towards a center 11 with the 2nd operation gestalt shown in this drawing 3 The counted value at that time (i), The authentication information (i, E (i, C1)) which

consists of both sides with the authentication child E (i, C1) who comes to sign with a key the joint sign (i, C1) which comes to join together the counted value (i) and the center ID code (C1) which specifies the center 11 of a transmission place is turned to a center 11, and it transmits. A user 10 After that, Counted value (i) is incremented and it considers as counted value (i+1).

[0032] In the item numbers 3, 5, and 8 shown in drawing 3 , moreover, a center 11 If an item number 3 is explained to an example about counted value The 1st subrule that it is counted value with a bigger value than the counted value (i-1) contained in the authentication information (i-1, E (i-1, C1)) to which the counted value (i) contained in the authentication information (i, E (i, C1)) transmitted this time has been transmitted last time, The counted value by which the authentication child E (i, C1) contained in authentication information (i, E (i, C1)) is contained in the authentication information (i, E (i, C1)) (i), When it investigates whether the Ruhr which consists of a subrule of both sides with the 2nd subrule that he is the same authentication child compared with the authentication child E (i, C1) who comes to carry out prominent to the joint sign (i, C1) which comes to join its own center ID code (C1) together with a key is followed and the Ruhr is followed The dispatch origin of the authentication information (i, E (i, C1)) attests that he is a user 10 surely. Moreover, since the dispatch origin of the authentication information is a valid user 10, a center 11 provides the user with service.

[0033] Each processing in the item numbers 9 and 10 shown in drawing 3 is only changed into the center ID code (C2) as which a center ID code specifies a center 12 compared with the processing in the item numbers 2, 4, 6, and 7 mentioned above, and the processing in item numbers 3, 5, and 8, respectively, and duplication explanation is omitted. With the 2nd operation gestalt shown in this drawing 3 , when sending authentication information towards centers 11 and 12 from a user 10, it specifies whether it is the authentication information sent to which addressing to a center, and the joint sign which consists of both sides of counted value and its destination (center ID code) is signed so that [that destination] it may not be altered. By carrying out like this, the authentication which was mistaken when the authentication information which the user 10 was going to send to the center 11 had been sent to the center 12 by the 3rd malicious person can be prevented.

[0034] In addition, if the 2nd operation gestalt explained with reference to drawing 3 is replaced with signing the counted value in the 1st operation gestalt with a key, and creating an authentication child, the joint sign with which it comes to combine counted value and a center ID code is signed with a key, an authentication child is created and only this point is changed, the modification of the 1st operation gestalt mentioned above etc. will be applied as it is. Therefore, the explanation beyond this about the 2nd operation gestalt is omitted here.

[0035] Drawing 4 is drawing showing the flow of the authentication method of the 3rd operation gestalt of this invention. In addition, the same number as item numbers 2-8 is attached and explained to drawing 4 among the item numbers 1-8 shown below.

1. The user 30 who shows premise drawing 4 , and centers 31 and 32 have the clock which gets to know current time, respectively. Moreover, the user 30 registers beforehand into centers 31 and 32 the key which signs the time of day by the user's 30 clock. On the other hand, centers 31 and 32 hold the access time of day obtained by authentication processing before basing on a user's 30 clock. moreover, the centers 31 and 32 -- centers 31 and 32 -- the access time of day to the centers 31 and 32 by each clock is held. In addition, the access time of day (tu02) to the access time of day (tu01) to a center 31 and the center 32 by a user's 30 clock differs mutually. Moreover, the access time of day (tc01) and the access time of day to the center 32 by the clock of a center 32 to the center 31 by the clock of a center 31 (tc02) also differ from each other

mutually. The access time of day tu01 and tc01 also usually differs. Similarly, the access time of day tu02 usually differs also from the access time of day tc02.

2. Authentication Request to Center 31 (the 1)

In receiving authentication, a user 30 turns to a center 31 the authentication information (tu1, E (tu1)) which consists of both sides with the authentication child E (tu1) who comes to sign with a key the time of day tu1 by the user's 30 clock (the 1st clock said to this invention), and its time of day tu1, and transmits.

3. Authentication Processing Center 31 in Center 31 is Time of Day Which Progressed ahead of Time of Day Tu01 Contained in Authentication Information (Tu01, E (Tu01)) to which Time of Day Tu1 Contained in Authentication Information (Tu1, E (Tu1)) Transmitted this Time Has been Transmitted Last Time. And the authentication child E (tu1) contained in the authentication information (tu1, E (tu1)) transmitted this time It investigates whether the Ruhr that he is the same authentication child compared with the authentication child who comes to sign with a key the time of day tu1 contained in the authentication information (tu1, E (tu1)) transmitted this time is followed. The current time which the time of day tu1 contained in the authentication information (tu1, E (tu1)) expresses further when the Ruhr is followed, The 1st elapsed time from current time which the time of day tu01 contained in the authentication information (tu01, E (tu01)) transmitted last time expresses (tu1-tu01), The receipt time tc1 of the authentication information (tu1, E (tu1)) which was acquired from the clock (the 2nd clock said to this invention) of a center 31 and which has been transmitted this time, The 2nd elapsed time (tc1-tc01) from the receipt time tc01 of the authentication information (tu01, E (tu01)) transmitted last time is compared. That is, when |(tu1-tu01)-(tc1-tc01) | (however, || shows an absolute value) is calculated and the count result is within a predetermined allowable error (for example, 30 seconds), the dispatch origin of the authentication information (tu1, E (tu1)) attests that he is a user 30 surely. Moreover, in the center 31, time of day tu1 and tc1 is recorded. Furthermore, since the dispatch origin of this authentication information is a valid user 30, the user 30 is provided with service.

[0036] Next, as a result of continuing at the processing mentioned above and performing an authentication demand, the case where a communication link goes wrong is explained.

4. Authentication Request to Center 31 (the 2)

In receiving authentication, a user 30 turns to a center 31 the authentication information (tu2, E (tu2)) which consists of both sides with the authentication child E (tu2) who comes to sign the time of day tu2 by the user's 30 clock, and its time of day tu2 with a key, and transmits. However, since this communication link goes wrong and there is no response from a center 31, in a user 30, that communications processing is judged to be a time-out, and requests authentication anew.

5. Authentication Request to Center 31 (the 3)

In receiving authentication, a user 30 turns to a center 31 the authentication information (tu3, E (tu3)) which consists of both sides with the authentication child E (tu3) who comes to sign the time of day tu3 by the user's 30 clock, and its time of day tu3 with a key, and transmits.

6. Investigate whether Authentication Processing Center 31 in Center 31 Follows Ruhr Which Authentication Information (Tu3, E (Tu3)) Transmitted this Time Mentioned above. The current time which the time of day tu3 contained in the authentication information (tu3, E (tu3)) expresses further when the Ruhr is followed, The 1st elapsed time from current time which the time of day tu1 contained in the authentication information (tu1, E (tu1)) transmitted last time expresses (tu3-tu1), The 2nd elapsed time (tc3-tc1) from the receipt time tc1 of the

authentication information (tu1, E (tu1)) transmitted last time [of the receipt time tc3 of the authentication information (tu3, E (tu3)) transmitted this time] acquired from the clock of a center 31 is compared. That is, when |(tu3-tu1)-(tc3-tc1) | (however, || shows an absolute value) is calculated and the count result is within a predetermined allowable error (for example, 30 seconds), the dispatch origin of the authentication information (tu3, E (tu3)) attests that he is a user 30 surely. Moreover, in the center 31, time of day tu3 and tc3 is recorded. Furthermore, since the dispatch origin of the authentication information is a valid user 30, the user 30 is provided with service.

[0037] Next, following on the processing mentioned above, the case where an authentication demand is given to centers 32 other than center 31 is explained.

7. Authentication Request to Center 32 (the 1)

In receiving authentication, a user 30 turns to a center 32 the authentication information (tu4, E (tu4)) which consists of both sides with the authentication child E (tu4) who comes to sign the time of day tu4 by the user's 30 clock, and its time of day tu4 with a key, and transmits.

8. Investigate whether Authentication Processing Center 32 of Center 32 Follows Ruhr Which Authentication Information (Tu4, E (Tu4)) Transmitted this Time Mentioned above. The current time which the time of day tu4 contained in the authentication information (tu4, E (tu4)) expresses further when the Ruhr is followed, The 1st elapsed time from current time which the time of day tu02 contained in the authentication information (tu02, E (tu02)) transmitted last time expresses (tu4-tu02), The 2nd elapsed time (tc4-tc02) from the receipt time tc02 of the authentication information (tu02, E (tu02)) transmitted last time [of the receipt time tc04 of the authentication information (tu4, E (tu4)) transmitted this time] acquired from the clock of a center 32 is compared. That is, when |(tu4-tu02)-(tc4-tc02) | (however, || shows an absolute value) is calculated and the count result is within a predetermined allowable error (for example, 30 seconds), the dispatch origin of the authentication information (tu4, E (tu4)) attests that he is a user 30 surely. Moreover, in the center 32, time of day tu4 and tc4 is recorded. Furthermore, since the dispatch origin of the authentication information is a valid user 30, the user 30 is provided with service.

[0038] Thus, in the authentication method of the 3rd operation gestalt of this invention, since the both sides of a user and a center are equipped with the clock, a user does not need to record the authentication child who sent for every center, and even when accessing a different center, he can perform an authentication request by the same device. Moreover, the authentication in a center may have an error between a user's clock and the clock of a center that only the time amount as the clock of a center with a user's same clock should be progressing. Moreover, by combining with the technique which is shown in drawing 2 and to which a center transmits a random number towards a user, even when safety can be raised further and a user's clock is reset by re-install of a user side system etc., it can be coped with.

[0039] In addition, in the 3rd operation gestalt explained with reference to drawing 4 , it replaces with signing only time of day with a key and creating an authentication child, and like the 2nd operation gestalt mentioned above, the joint sign with which it comes to combine time of day and a center ID code may be signed with a key, and an authentication child may be created. If it carries out like this, the authentication which was mistaken when the authentication information which should be transmitted to a center 31 reached a center 32 can be prevented.

[0040]

[Effect of the Invention] As explained above, according to the authentication method of this invention, the authentication in a center It is the sign located after the sign by which the 1st sign

contained in the 1st authentication information transmitted this time was contained in the 2nd authentication information transmitted last time. And since the 1st authentication child contained in the 1st authentication information is made based on the Ruhr that he is the same authentication child compared with the authentication child who comes to sign with a key the 1st sign (or joint sign with which it comes to combine the 1st sign and center ID code) contained in the 1st authentication information, Even if it is the case where an authentication child does not reach a center, authentication processing can be performed easily succeedingly. Moreover, a user does not need to record the authentication child who sent for every center, and even when accessing a different center, he can perform authentication processing by the same device.

[Brief Description of the Drawings]
[Drawing 1] It is drawing showing the flow of the authentication method of the 1st operation gestalt of this invention.
[Drawing 2] In the authentication method shown in drawing 1 , when a center receives an authentication request, it is drawing having shown processing when the counted value from a user is smaller than the counted value recorded on the center.
[Drawing 3] It is drawing showing the flow of the authentication method of the 2nd operation gestalt of this invention.
[Drawing 4] It is drawing showing the flow of the authentication method of the 3rd operation gestalt of this invention.
[Drawing 5] It is drawing showing the flow of the authentication method of the conventional challenge response mold.
[Drawing 6] It is drawing showing the flow of the authentication method of the challenge response mold proposed by JP,5-219053,A.
[Description of Notations]
10 30 User
11, 12, 31, 32 Center